N° d'ordre : 12/2021-D/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediène
USTHB
Faculté de Mathématiques, département d'Algèbre

THESE

Présentée pour l'obtention du grade de **Doctorat en Sciences**
en **MATHEMATIQUES**
Spécialité : **Algèbre et Théorie des Nombres**
Par : **YOUMBAI Ahmed El Amine**

Sujet

Rang de Courbes Elliptiques

Soutenue publiquement, le 04/07/2021, devant le jury composé de

M. BETINA, Kamel	Professeur à l'USTHB	Président
M. BEHLOUL, Djilali	Professeur à l'USTHB	Rapporteur
M. REZAOUI, Mohamed Salem	Maître de Conférence /A à l'USTHB	Examinateur
M. AIT AMRANE, Lyes	Maître de Conférence /A à l'ESI Oued Smar	Examinateur
M. AHMIA, Moussa	Maître de Conférence /A à l'Université de Jijel	Examinateur
M. GUERBOUSSA, Yacine	Maître de Conférence /A à l'UKMO, Ouargla	Examinateur

Titre : Rang de Courbes Elliptiques

Résumé :
Cette thèse examine certaines approches sur le rang des courbes elliptiques et ses interventions dans la résolution des équations Diophantiennes. Elle donne aussi un bel exemple de la façon d'utiliser la théorie et les logiciels existants pour étudier toute famille de courbes elliptiques paramétrées sur le corps de fonctions $\mathbb{Q}(t)$. Nous avons utilisé la théorie des courbes elliptiques pour améliorer les résultats dans [45, 50] concernant les solutions rationnels des équations diophantiennes $f(x)^2 \pm f(y)^2 = z^2$ en ramenant le problème à chercher des points d'ordre infini sur certaines familles de courbes elliptiques sous un modèle quartique, puis, via la théorie élémentaire des nombres nous avons résolu complètement le problème. Dans une seconde partie de cette thèse, l'un de nos principaux résultats est la construction de quelques familles infinies de courbes elliptiques à un et deux paramètres ayant un rang ≥ 5 et cela à partir du modèle $(y-h)(y-h) = (x-a)(x-b)(x-c)$ plus général que celui dans [49]. Par spécialisation, des courbes elliptiques de grand rang (7, 8, 9, 10 et 11) sur $\mathbb{Q}$ on été obtenues.

Mots clés : Courbe Elliptiques, Groupe de Mordell-Weil, Rang, Equations Diophantiennes.

Université des Sciences et Technologie Houari Boumedienne, Faculté de Mathématiques.
Laboratoire : Algèbre et Théorie des Nombres (LATN)-USTHB

Title : Rank of Elliptic Curves

Abstract :
This thesis examines some approaches on the rank of elliptic curves and its interventions in the resolution of Diophantine equations. It also gives a good example of how to use existing theory and software to study any parametric family of elliptic curves over the function field $\mathbb{Q}(t)$. We used the theory of elliptic curves to improve the results in [45, 50] concerning the rational solutions of the diophantine equations $f(x)^2 \pm f(y)^2 = z^2$ by using an appropriate transformations to reduce the problem to finding points of infinite order on some families of elliptic curves under a quartic model, and then, using elementary number theory we solved the problem completely. In a second part of this thesis, one of our main results is the construction of some infinite families of one- and two-parameter elliptic curves having a rank ≥ 5 and this from the model $(y-h)(y-h) = (x-a)(x-b)(x-c)$ more general than the one in [49]. By specialisation, elliptic curves of large rank (7, 8, 9, 10 and 11) over $\mathbb{Q}$ have been obtained.

Keywords : Elliptic Curves, Mordell-Weil Group, Rank, Diophantine Equations.

USTHB : University of Sciences and Technologie Houari Boumedienne, Faculty of Mathematics.
Laboratory : Algèbre et Théorie des Nombres (LATN)-USTHB

à Mohammed Laid $\begin{cases} YOUMBAI \\ TIDJANI \end{cases}$

Remerciement

Je tiens à remercier vivement le professeur Djilali BEHLOUL, pour la confiance qu'il m'a témoigné en acceptant la direction scientifique de mes travaux. Je lui suis reconnaissant de m'avoir fait bénéficier tout au long de ce travail de sa grande compétence, de sa rigueur intellectuelle, de son dynamisme, et de son efficacité.

Je suis très honoré à remercier de la présence à mon co-directeur de thèse Monsieur A. Muhammed ULUDAG, chef de département de Mathématiques à l'université de Galatasaray (Turquie), pour l'honneur qu'il m'a fait en acceptant de m'accueillir dans son laboratoire.
Profonde reconnaissance pour l'intérêt qu'il porte à ce travail.

Je tien également à remercier les membres du jury de cette thèse pour leur participation et pour toutes remarques intéressantes, pour le temps consacré à la lecture de ce travail ainsi que pour les commentaires m'ayant permis de l'améliorer.

Je remercie Monsieur Mohamed Moumen Bekkouche, pour son amitié, son soutien et pour son intérêt permanent à mon égard.

A titre plus personnel, Je remercie chaleureusement mon épouse, Ilham , pour la grande patience, l'encouragement et la confiance qu'elle m'a témoignée dont elle a fait preuve à son soutien moral.
Finalement je remercie mes parents pour leurs soutiens qui m'a été bien utile durant ma thèse.

Table des matières

Introduction

Parmi les questions fondamentales que l'on puisse se poser à propos des courbes elliptiques est

Question 1. *Quels groupes abéliens apparaissent comme le groupe d'une courbe elliptique définie sur les rationnels ?*

Par des résultats bien connus de Mordell (généralisés à d'autres corps de nombres par Weil) et de Mazur (généralisés de manière similaire par Merel), nous savons que les groupes sont de type finie et que les sous-groupes de torsion doivent être l'un des quinze groupes possibles déterminés par Mazur et Chaque possibilité peut être réalisée. Ce qui n'est pas connu, c'est la taille de la partie libre du groupe, plus précisément le rang du groupe d'une courbe elliptique. La plupart des spécialistes croient que pour chaque entier positif m, il existe une courbe elliptique définie sur $\mathbb{Q}$ dont le groupe de Mordell-Weil a un rang supérieur à m. Une autre question naturellement liée pour laquelle il n'y a pas suffisamment d'arguments pour fournir une conjecture raisonnable est

Question 2. *Pour tout entier positif m et possible groupe de torsion T, existe-t-il une courbe elliptique dont le groupe a un rang supérieur à m et dont le sous-groupe de torsion est T ?*

Même si nous pouvions répondre à ces questions, nous aimerions quand même produire des exemples de telles courbes.
Cette thèse passe en revue certaines techniques utilisées pour construire des familles infinies de courbes elliptiques sur les corps de fonctions $\mathbb{Q}(t)$ et $\mathbb{Q}(t,k)$ de rang générique[1] élevé. Ensuite, nous pouvons obtenir par spécialisation des courbes elliptiques définies sur $\mathbb{Q}$ de grand rang.
La complexité de la construction d'une courbe elliptique de grand rang varie selon les méthodes employées et la plupart d'entre-elles ne s'appliquent que pour des modèles de courbes précis (pas nécessairement de Weierstrass). La difficulté de produire des exemples de courbes elliptiques de rang élevé varie selon le sous groupe de torsion, des records du rang ont été établis pour chaque sous groupe de torsion et nous constatons que plus son cardinal augmente le record du rang est petit comme nous pouvons le voir dans le tableau suivant dont les données son collectées du fameux site web de Andrej Dujella [11].

1. la valeur r_0 pour laquelle toute spécialisation donne une courbe elliptique de rang $\geq r_0$

TABLE 1 – Records du Rang

$\mathbb{T}$	$B(\mathbb{T})$	Auteurs
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	20	Elkies - Klagsbrun (2020)
$\mathbb{Z}/3\mathbb{Z}$	15	Elkies - Klagsbrun (2020)
$\mathbb{Z}/4\mathbb{Z}$	13	Elkies - Klagsbrun (2020)
$\mathbb{Z}/5\mathbb{Z}$	9	Klagsbrun (2020)
$\mathbb{Z}/6\mathbb{Z}$	9	Klagsbrun (2020), Voznyy (2020)
$\mathbb{Z}/7\mathbb{Z}$	6	Klagsbrun (2020)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006), Dujella - MacLeod - Peral (2013)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009), van Beek (2015)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006), Fisher (2016)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	9	Dujella - Peral (2012,2019), Klagsbrun (2020)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006), Dujella - Peral - Tadic (2015), Dujella - Peral (2020)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000,2001,2006,2008), Campbell - Goins (2003), Rathbun (2003,2006,2013), Dujella - Rathbun (2006), Flores - Jones - Rollick - Weigandt - Rathbun (2007), Fisher (2009)

$\mathbb{T}$	$G(\mathbb{T})$	Auteurs
0	18	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	11	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	7	Elkies (2007)
$\mathbb{Z}/4\mathbb{Z}$	5	Kihara (2004), Elkies (2007), Dujella - Peral - Tadic (2014) Khoshnam - Moody (2016)
$\mathbb{Z}/5\mathbb{Z}$	3	Lecacheux (2001), Eroshkin (2009), MacLeod (2014)
$\mathbb{Z}/6\mathbb{Z}$	3	Lecacheux (2001), Kihara (2006), Eroshkin (2008), Woo (2008), Dujella - Peral (2012,2020), MacLeod (2014,2015)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2009), MacLeod (2014)
$\mathbb{Z}/8\mathbb{Z}$	2	Dujella - Peral (2012), MacLeod (2013)
$\mathbb{Z}/9\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/10\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/12\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	7	Elkies (2007)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	4	Dujella - Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	2	Dujella - Peral (2012,2015,2017), MacLeod (2013)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0	Kubert (1976)

où $\mathbb{T}$ désigne le sous groupe de torsion.

$B(\mathbb{T}) = \sup\{rang(E(\mathbb{Q})) :$ le sous groupe de torsion de E sur $\mathbb{Q}$ est $\mathbb{T}\}$.

$G(\mathbb{T}) = \sup\{rang(E(\mathbb{Q}(t))) :$ le sous groupe de torsion de E sur $\mathbb{Q}(t)$ est $\mathbb{T}\}$.
Cette thèse comporte 5 chapitres :
Le premier chapitre contient un rappel sur l'arithmétique des courbes elliptiques.
Le second chapitre est consacré au rang de courbes elliptiques, nous présentons quelques techniques connues pour construire des courbes elliptiques de grand rang sur les corps de fonctions ou plus particulièrement celui des rationnels, suivi d'exemples illustrant la façon dont on applique ces techniques.
Dans le chapitre 3, Un bel exemple est donné, montrant comment utiliser les logiciels et la théorie existante pour étudier les courbes elliptiques paramétrées. Dans cet exemple, la courbe est à deux paramètres donnée par l'équation

$$y^2 = x^3 + a^2x^2 - (a^2 + b^2)x + b^2.$$

Dans le Chapitre 4, nous mettons en relation la résolution de quelques équations Diophantiennes de la forme

$$f(x)^2 \pm f(y)^2 = z^2$$

et le rang de certaines courbes elliptiques sous un modèle quartique. Via la théorie des courbes elliptiques nous donnons une réponse positive à la question posée par M. Ulas et A. Togbé dans [45], puis, nous résolvons complètement le problème en utilisant seulement la théorie élémentaire des nombres.
Le dernier chapitre est consacré à l'étude de la courbe elliptique paramétrée

$$E_{(a,b,c)} : (y - h)(y + h) = (x - a^\alpha)(x - b^\beta)(x - c^\gamma),$$

où $a, b, c \in \mathbb{Q}(t)$ ou $\mathbb{Q}(t, k)$, $h = a^l b^m c^n$ et (l, m, n, α, β et γ sont des entiers positifs).
Suivant une méthode itérative, nous construisons :
• Deux familles infinies de courbes elliptiques de rang au moins 5 sur $\mathbb{Q}(t, k)$.
• Deux familles infinies de courbes elliptiques de rang au moins 5 sur $\mathbb{Q}(t)$ induites par les bords d'un cuboïdes rationnel.
• Une famille infinie de courbes elliptiques de rang au moins 5 sur $\mathbb{Q}(t)$ induite par des triplets Diophantiens rationnels de la forme $\{1, a^2, b^2\}$.
Par spécialisation, nous avons obtenu des courbes elliptiques sur le corps des rationnels de rang élevé allant jusqu'à (7,8,9,10 et 11).
Nos principaux résultats [47, 48], sont des travaux originaux publiés dans :
Periodica Mathematica Hungarica.
Hacettepe Journal of Mathematics and Statistics.

Chapitre 1

Arithmétiques des Courbes Elliptiques

Dans ce chapitre, nous définissons brièvement les notions fondamentales des courbes elliptiques qui se trouvent principalement dans les ouvrages [40, 22, 46].

1.1 Courbes Algébriques

1.1.1 Espace Affine, Projectif

Soit K un corps et $\overline{K}$ une clôture algébrique de K.

Définition 3. *Un n-espace Affine sur K est l'ensemble des n-uples*

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{(a_1, ..., a_n) : a_i \in \overline{K}\}.$$

L'ensemble des points K-rationnels de $\mathbb{A}^n$ est

$$\mathbb{A}^n(K) = \{(a_1, ..., a_n) : a_i \in K\}.$$

Pour tout ensemble S de fonctions à coordonnées dans l'anneau $K[\mathbb{A}^n]$ il y a un sous ensemble affine $Z(S)$ contenu dans $\mathbb{A}^n$ qui est l'annulateur de S.

$$Z(S) = \{(a_1, ..., a_n) \in \mathbb{A}^n : f(a_1, ..., a_n) = 0 \text{ pour tout } f \in S\}$$

Définition 4. *Un sous ensemble V de $\mathbb{A}^n$ est un ensemble algébrique affine si $V = Z(S)$ pour certain $S \subseteq K[\mathbb{A}^n]$.*

Définition 5. *Un sous ensemble Y d'un espace topologique qui ne peut pas se décomposé en deux sous ensembles propres Y_1 et Y_2 fermés dans Y est dit irréductible.*

Définition 6. *Une variété algébrique affine est un sous ensemble algébrique affine irréductible de $\mathbb{A}^n$.*

Pour $n = 2$, c'est une courbe plane, elle est définie par un seul polynôme à deux variables.

Définition 7. *Un n-espace projectif $\mathbb{P}^n$ sur K est l'ensemble des lignes qui passent par l'origine dans A^{n+1}*

$$\mathbb{P}^n = \frac{\mathbb{P}^n(\overline{K}) = \{(a_1, ..., a_n) \in \mathbb{A}^{n+1} : \text{ les } a_i \text{ ne sont pas tous nuls}\}}{\sim},$$

où $\sim$ est une relation d'équivalence définie par

$$(x_0 : ... : x_n) \sim (y_0 : ... : y_n) \Leftrightarrow (x_0 : ... : x_n) = \lambda(y_0 : ... : y_n), \lambda \in \overline{K}^*.$$

Les courbes algébriques peuvent être classifiées par un invariant dit le genre, si la courbe est lisse de degré d son genre est donné par le

Théorème 8. *Soit C est une courbe plane, connexe de degré $d > 0$ et contenue dans l'espace projectif $\mathbb{P}^2$. Alors*

$$g = \frac{(d-2)(d-1)}{2}$$

et pour tout $d > 0$, il existe une telle courbe.

De là on constate que les droites et les coniques sont de genre 0, tant dit que les cubiques non singulières (l'objet de notre étude) sont de genre 1. Le genre représente aussi une mesure de complexité des courbes algébriques, tel que défini dans le théorème de Rieman-Roch (voir [19]), les plus simples des courbes algébriques lisses sont ceux du genre 0. En effet, les droites sont totalement paramétrables tout comme les coniques possédants un point K-rationnel comme le montre le résultat suivant :

Théorème 9. *Si C est une conique définie sur K et que $C(K)$ n'est pas vide, alors $C(K)$ est isomorphe à $\mathbb{P}^1(K)$.*

Ce théorème dit que nous pouvons paramétrer les solutions de n'importe quel modèle de coniques, tant qu'il y a au moins une solution.
Notons aussi qu'une courbe plane de genre 2 ou plus (Hyperelliptique : courbe algébrique plane d'équation $y^2 = f(x)$ pour $f(x)$ de degré $n > 3$) n'admet qu'un nombre fini de points rationnels.

1.2 Courbes Elliptiques

Soit K un Corps de nombres

Définition 10. *Une courbe elliptique E sur le corps K est la donnée d'une paire (E, O) où E est une courbe algébriques plane de genre 1 et O le point à l'infini.*

Dans le plan projectif $\mathbb{P}^2$ ayant un point O sur la droite à l'infini ; après avoir mis à l'échelle X et Y, nous avons l'équation projective de Weierstrass de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1}$$

où les $a_i \in \overline{K}$.
On trouve le point à l'infini O en mettant $Z = 0$ dans (1.1) ce qui entraine $X = 0$ et Y quelconque, d'où le point à l'infini $O = (0 : Y : 0) = (0 : 1 : 0)$ est le seul point $\overline{K}$-rationnel sur la ligne à l'infini $Z = 0$. De plus O est un point d'inflexion non singulier, la tangente étant la droite à l'infini. Pour facilité la notation, nous pouvons tout de même travailler avec le modèle affine de la courbe, cela peut être effectuer avec le changement de variables $x = \dfrac{X}{Z}$ et $y = \dfrac{Y}{Z}$ pour obtenir la forme affine non homogène de l'équation de Weierstrass pour une courbe elliptique

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2}$$

Les courbes elliptiques peuvent être considérées comme des courbes de complexité d'un niveau supérieur à celles des coniques. Une courbe elliptique E définie sur un corps K est une courbe lisse de genre 1 avec au moins un point K-rationnel. Contrairement à notre compréhension relativement complète des coniques, notre compréhension des courbes elliptiques est assez minime.
les courbe

1.2.1 Quelques Invariants Relatifs aux Courbes Elliptiques

Soit E une courbe elliptique sur le corps K donnée par l'équation de Weierstrass (modèle général)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.3}$$

Nous définissons quelques notations standards afin de simplifier l'équation (1.3) pour des raison purement calculatoire.

Si la caractéristique du corps K est différente de 2 alors, pour

$$Y = \frac{1}{2}(y + \frac{a_1}{2}x + \frac{a_3}{2}), \tag{1.4}$$

on a

$$Y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{1.5}$$

où

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6. \end{aligned} \tag{1.6}$$

Si De plus la $carat(K) \neq 3$ alors, on peut éliminer le monôme en x^2 dans (1.5) et rendre le polynôme du second membre unitaire par les changements de variables

$$X = \frac{x + 3b_2}{36}$$

$$Y = \frac{y}{108}$$

pour obtenir

$$Y^2 = X^3 - 27c_4X + 54c_6, \tag{1.7}$$

avec

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned} \tag{1.8}$$

Posons maintenant

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Définition 11. *Le discriminant d'une cubique de Weierstrass est donné par le polynôme homogène*

$$\triangle = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8 \tag{1.9}$$

Les cubiques peuvent être classifiées par le discriminant :

• Si $\triangle = 0$, alors la cubique est singulière.

• Si $\triangle \neq 0$, alors il s'agit d'une courbe elliptique.
• Si $\triangle < 0$, la courbe elliptique est connexe.
• Si $\triangle > 0$, la courbe elliptique est la réunion de deux composantes connexes.
Pour $Carac(K) \neq 2, 3$ nous avons également l'invariant suivant :

Définition 12. *Le j-invariant d'une courbe elliptique E sur le corps K est l'élément de K égale à :*

$$j(E) = \frac{c_4^3}{\triangle}. \tag{1.10}$$

Désormais, lorsqu'on travail sur un corps de caractéristique $\neq 2, 3$ nous pouvons supposer que notre courbe peut s'écrire sous le modèle réduit de Weierstrass

$$y^2 = x^3 + ax + b$$

Dans ce cas là, le discriminant $\triangle$ et le j-invariant son donnés par

$$\triangle = -16(4a^3 + 27b^2), \quad j = 1728\frac{(4a)^3}{\triangle}$$

1.2.2 Loi du Groupe sur une Cubique

L'idée de construire une loi de groupe sur une cubique projective remonte à 1835 quand Jacobi dans [23] a proposé pour la première fois l'utilisation d'une loi de groupe sur une courbe cubique projective. Au premier lieu, l'idée était de tracé à partir d'un point rationnel P d'une cubique E la tangente pour en obtenir un autre point rationnel Q (qui est le troisième point d'intersection de la tangente avec E), puis continuer le processus avec Q et ainsi de suite. Mais, Comme cela ne donne pas une loi de groupe, le choix du point rationnel O comme élément neutre et la loi géométrique corde-tangente nous permet de définir une loi de groupe $P + Q$ comme suite.
Soit E une courbe elliptique donnée par une équation de Weierstrass, elle peut être considérée aussi comme une courbe projective dans $\mathbb{P}^2$ ($E \subset \mathbb{P}^2$) formée de points $P = (x, y)$ satisfaisant l'équation de E plus le point à l'infini $(0 : 1 : 0)$.
Comme E est de degré 3 et d'après le théorème d'intersection de Bezout, si E intersecte une droite projective L en deux points P, Q alors il existe forcément un troisièmement point d'intersection R (pas nécessairement distincts si L est une tangente de E).
Nous définissons une loi de groupe sur E selon la règle géométrique suivante :
Soient P et Q deux points de E, L la droite qui passe par ces deux points (tangente si $P = Q$) et R le troisième point d'intersection de L avec E. Soit L' la droite passante par R et O. Alors $P + Q$ est le points tel que L' intersecte E en R, O et $P + Q$

1.3 Groupe de Mordell-Weil

Si nous essayons de paramétrer les points K-rationnels sur une courbe elliptique de la manière dont nous paramétrons les points K-rationnels sur une conique, nous découvrons que (en général) ce n'est pas possible. Toutefois, on peux considéré sur cette dernière la loi du groupe définie précédemment. Une question fondamentale que nous posons alors est :

Question 13. *Quels groupes peut être $E(K)$?*

Pour $K = \mathbb{Q}$ nous avons le théorème important suivant, dû à Mordell et à Weil pour les variétés abéliennes sur les corps de nombres K.

Théorème 14 (Mordell)**.** *Le groupe abélien $E(\mathbb{Q})$ est de type fini*

$$E(\mathbb{Q}) \simeq \mathbb{T} \oplus L, \tag{1.11}$$

où $\mathbb{T}$ est un sous groupe fini (les éléments de torsion) et L une partie libre isomorphe à $\mathbb{Z}^r$ ($\mathbb{Z}$-module libre de rang r).

Ce théorème affirme qu'à partir d'un nombre fini de points $\mathbb{Q}$-rationnels d'une courbe elliptique $E(\mathbb{Q})$ on peut générer tout les points de la courbe.

Définition 15. *l'entier non négatif r est le rang de la courbe elliptique E.*

Weil a prouvé que le groupe $E(K)$ est en fait de type fini pour n'importe quel corps de nombre K. Ce fait a depuis été étendu à d'autres corps (voir [40], section III.6) ; en particulier, $E(\mathbb{Q}(t))$ est de type fini.
En outre, Mazur a prouvé que le sous groupe de torsion d'une courbe elliptique sur le corps des rationnel $\mathbb{Q}$ ne peut être isomorphe qu'à l'un des quinze groupes suivants

$$\mathbb{T}(\mathbb{Q}) = \begin{cases} \frac{\mathbb{Z}}{n\mathbb{Z}} & 1 \leq n \leq 10 \text{ ou } n = 12, \\ \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{(2n)\mathbb{Z}} & 1 \leq n \leq 4, \end{cases} \tag{1.12}$$

et que chacun se présente comme le sous-groupe de torsion d'une courbe elliptique.
Merel a depuis étendu ce théorème et prouvé la forte conjecture de la borne uniforme : si K est un corps de nombres, alors l'ordre du sous-groupe de torsion de $E(K)$ est borné par une constante qui ne dépend que du degré de K sur $\mathbb{Q}$.
Ces théorèmes de Mordell, Weil, Mazur et Merel nous ont donné une bonne idée du problème et amené très loin dans la réponse à la question de savoir quels peuvent être

les groupes $E(K)$, mais ils n'y répondent pas complètement à la question et jusqu'à présent aucune formule ou algorithme ne peut garantir le calcul de la taille exact de la partie libre du groupe de Mordell-Weil d'une courbe elliptique. En particulier, nous ne savons pas quelles valeurs du rang sont possibles pour les courbes elliptiques ni dans le cas de courbes elliptiques définies sur un corps général K, ni dans le cas plus spécifique de $K = \mathbb{Q}$. Une grande question ouverte dans la théorie des courbes elliptiques est de savoir si le rang est borné ou non.
La démonstration du fameux théorème de Mordell-Weil se fait en deux étapes distincts.
• **Etape 1 :** Appelée aussi la version faible du théorème de Mordell, il s'agit de montrer que le quotient $\frac{E(\mathbb{Q})}{nE(\mathbb{Q})}$ est fini, en particulier nous pouvons voir que le groupe quotient $\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}$ est fini :

Proposition 16. *Le groupe quotient $\frac{E(K)}{2E(K)}$ est fini.*

Démonstration. On utilise des homomorphismes de groupes abéliens :

$$\theta_i : E(K) \longrightarrow \frac{K^*}{K^{*2}}$$

dont les noyaux satisfont la relation :

$$\bigcap_{i=1}^{3} \theta_i \subset 2E(K)$$

L'équation de Weierstrass de la courbe E est de la forme :

$$E(K) : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

Pour caractéristique de K différent de 2 et 3, les fonctions θ_i prennent les valeurs :

$$\begin{cases} \theta_i(O_E) = 1 \\ \theta_i(x, y) = e_i \text{ si } x \neq e_i \\ \theta_i(e_i, 0) = (e_i - e_j)(e_i - e_k) \end{cases}$$

Pour d'autres détails consulter [40]. □

• **Etape 2 : (Hauteurs)** Le but de cette étape est de passer du théorème faible de Mordell-Weil au théorème fort de Mordell-Weil (14).
Le Théorème affirme qu'il existe un ensemble fini de points sur E à partir duquel tous les autres points peuvent être obtenus en traçant à plusieurs reprises des lignes tangentes et des lignes passant par des points, comme dans la définition de la loi du

groupe. En admettons l'étape 1 (le théorème faible de Mordell-Weil) nous avons $E(\mathbb{Q})/2E(\mathbb{Q})$ est fini. Cela seul ne suffit pas pour en déduire le résultat le plus fort. Par exemple, $\mathbb{R}/2\mathbb{R} = 0$, donc est fini, même si $\mathbb{R}$ n'est pas de type fini. Dans notre cas, supposons que nous ayons les points $R_1, ..., R_n$ représentant le nombre fini de classes dans $E(\mathbb{Q})/2E(\mathbb{Q})$. Soit $P \in E(\mathbb{Q})$ un point arbitraire. Nous pouvons écrire

$$P = R_i + 2P_1$$

pour certain i et P_1. puis nous écrivons P_1 d'une manière similaire sous la forme

$$P_1 = R_j + 2P_2,$$

et ainsi de suite...
Si nous pouvons prouver que le processus s'arrête, alors nous pouvons remettre les choses ensemble et obtenir le théorème. La théorie des hauteurs montrera que les points $P_1, P_2, ...$ deviennent plus petits, dans un certain sens, de sorte que le processus finira par produire un point P_k qui se trouve dans un ensemble fini de petits points. Ces points, avec les R_i, donnent les générateurs de $E(\mathbb{Q})$.
Nous introduisons des fonctions particulières : les hauteurs sur les groupes abéliens.

Définition 17. *Une hauteur sur un groupe abélien A est une fonction à valeurs réelles sur A*

$$h : A \longrightarrow \mathbb{R}$$

qui satisfait les trois axiomes :
(h1) *Soit un point P_0 de A ; alors il y a une constante réelle $c_0 = c_0(P_0, A)$ telle que :*

$$h(P_0 + P) \leq 2h(P) + c_0, \qquad (\forall P \in A).$$

(h2) *Il y a un entier $m \geq 2$ et une constante $c_1 = c_1(A)$ tels que :*

$$h(mP) \geq m^2 h(P) - c_1, \qquad (\forall P \in A).$$

(h3) *Pour toute constante c, l'ensemble des points de hauteur bornée par c :*

$$\{P \in A, h(P) < c\}$$

est fini.

Une telle fonction hauteur n'est pas unique, elle est déterminée par sa valeur $h(P)$:

hauteur logarithmique, hauteur de Weil, hauteur canonique, hauteur locale, etc...

Proposition 18. *Soit un groupe abélien A tel que le groupe quotient A/mA soit fini. Alors le groupe A est de type fini.*

Démonstration. Nous utilisons un algorithme de descente infinie pour construire une suite infinie $P, P_1, ..., P_n, ...$ de points de A. Choisissons des représentants $T_1, ..., T_r$ des classes A/mA. Soit un point $P \in A$ égal à la combinaison linéaire

$$P = mP_1 + T_{i_1} \quad (1 \leq i_1 \leq r). \tag{1.13}$$

De même le point P_1 est une combinaison linéaire

$$P_1 = mP_2 + T_{i_2} \quad (1 \leq i_2 \leq r). \tag{1.14}$$

En continuant de cette manière, nous obtenons une suite de points $P_i \in A$:

$$\begin{aligned} P_j &= mP_{j+1} + T_{i_{j+1}} \quad (1 \leq i_{j+1} \leq r), \\ ... &= ..., \\ ... &= ..., \\ P_{n-1} &= mP_n + T_{i_{n-1}} \quad (1 \leq i_{n-1} \leq r). \end{aligned}$$

Appliquons à la relation :

$$P_j - T_{i_{j+1}} = mP_{j+1} \tag{1.15}$$

l'axiome ***(h1)*** à gauche et l'axiome ***(h2)*** à droite

$$h(P_j) \leq \frac{1}{m^2}[2h(mP_{j-1} + 1) + c_j] \tag{1.16}$$

Additionnons membre à membre les inégalités (1.16) de P à P_n. Nous obtenons l'inégalité :

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + ... + \frac{2^{n-1}}{m^{2n}}\right), \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{c_4}{m^2 - 2}. \end{aligned} \tag{1.17}$$

L'hypothèse $m \geq 2$ implique : $\dfrac{2}{m^2} \leq 2$.

La formule (1.17) implique l'inégalité :

$$h(P_n) \leq \frac{h(P)}{2^n} + \frac{c_4}{2} < 1 + \frac{c_4}{2}. \tag{1.18}$$

L'axiome ***(h3)*** appliqué à l'inégalité (1.18) implique que l'ensemble $\{P_n\}$ est fini.

$$\{P_n\} = \{B_1, B_2, ..., B_N\}. \tag{1.19}$$

Les représentants des classes $T_1, ..., T_r$ et les relations (1.13) et (1.19) impliquent que tout élément $P \in A$ est une combinaison linéaire de la forme :

$$P = k_1T_1 + ... + k_1T_1 + l_1B_1 + ... + l_NB_N. \tag{1.20}$$

Ce qui prouve que le groupe abélien A est de type fini. □

Cette méthode est la descente infinie sur une courbe elliptique. Un bel exemple de l'utilisation d'une fonction hauteur ce trouve dans [4].

1.3.1 Régulateur

Soit E une courbe elliptique sur $\mathbb{Q}$ définie sous sa forme affine $y^2 = x^3 + Ax + B$.

Définition 19. *Si $P = (x, y) \in E(\mathbb{Q})$, $x = \frac{a}{b}$; $(a, b) = 1$, on appelle hauteur naïve de P la quantité :*

$$h(P) = \log\left(\max(|a|, |b|)\right) \geq 0.$$

Par convention $h(\infty) = 0$.

Proposition 20. *Il existe une unique fonction $\hat{h}$*

$$\hat{h} : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

vérifiant :
i) *$\hat{h}(P) - h(P)$ borné.*
ii) *$\hat{h}(2P) = 4\hat{h}(P)$.*

Cette fonction est définie par : $\hat{h}(P) = \lim_{n\to\infty} \dfrac{h(2^nP)}{4^n}$

Définition 21. *La fonction $\hat{h}$ est appelée la fonction hauteur canonique.*

Soit E une courbe elliptique définie sur $\mathbb{Q}$ de rang r , $P_1, P_2, ..., P_r$ les générateurs du groupe $E(\mathbb{Q})$.

Définition 22. *Le régulateur $R(E)$ de la courbe elliptique E est le déterminant de la matrice :*

$$(\langle P_i, P_j \rangle) \text{ avec } 1 \leq i, j \leq r$$

où

$$\langle P_i, P_j \rangle = \frac{1}{2}(\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P)_j)$$

($\hat{h}$ étant la fonction hauteur canonique).

En particulier, si $P_1, P_2, ..., P_n$ sont des points d'une courbe elliptique E, on a le résultat suivant

Proposition 23. *Si $R(\{P_1, P_2, ..., P_n\}) \neq 0$ alors les points $P_1, P_2, ..., P_n$ sont linéairement indépendants.*

Dans le cas où les points sont tous d'ordre infini, leur régulateur implique une borne inférieure du rang de la courbe elliptique E.

1.3.2 Courbe Elliptique sur un Corps Fini

Ici, nous abordons les courbes elliptiques définies sur les corps finis, l'aspect le plus important relié a une telle courbe est leur nombre de points rationnels. Si E est une courbe elliptique définie sur le corps fini K (a q éléments) et si $x \in K$, il y a au plus deux valeurs de y satisfaisant l'équation de E. On a donc évidemment

$$|E(K)| \leq 2q + 1$$

qui d'après Hasse égal aproximativement à q pour une courbe elliptique définie sur un corps fini à q éléments bien-sur avec une marge d'erreur qui ne doit pas dépassé $2\sqrt{q}$

Théorème 24 (Hasse)**.** *On a l'inégalité suivante :*

$$|q + 1 - |E(K)|| \leq 2\sqrt{q}$$

Le théorème de Hasse permet parfois de déterminer facilement l'ordre de $E(K)$ si l'on parvient à détecter un point de $E(K)$ d'ordre d assez grand, en effet, le comptage des multiples de ce point laisse un petit nombre de possibilités pour l'ordre de $E(K)$.
Nous allons voir plus loin, qu'il est expérimentalement connu et fortement soutenu par la conjecture BSD qu'on peux espérer d'avoir une courbe elliptique de grand rang parmi c'elles qui ont un groupe de Mordell–Weil contenant beaucoup de points sur plusieurs corps finis.

1.4 Corps de Fonctions et Théorème de spécialisation de Silverman

Soit K un corps de nombres rationnels et V une variété définie sur K.
On peut définir une courbe elliptique E sur le corps de fonctions $K(V)$ par l'équation de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.21}$$

où les $a_i \in K(V)$ sont définis en presque tout les points $t \in V$. Il serait Donc Possible de définir une spécialisation de la courbe elliptique E en t par :

$$E : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t). \tag{1.22}$$

De même, si $P = (x, y)$ est un point de $E(K(V))$, alors les fonction $x, y \in K(V)$ seront définis pour presque tout $t \in V$. Donc, on peut également spécialiser P au point $P = (x(t), y(t))$. Sachant que le théorème de Mordell–Weil reste valable pour les corps de fonctions, on peut définir un homomorphisme de spécialisation pour presque tout $t \in V$

$$\sigma_t : E(K(V)) \longrightarrow E_t. \tag{1.23}$$

Théorème 25 (Silverman)**.** *Soit C une courbe définie sur K, et E une courbe elliptique définie sur $K(C)$. Alors, l'application de spécialisation*

$$\sigma_t : E(K(C)) \longrightarrow E_t$$

est bien définie et injective.

Ce théorème nous sera très utile dans la suite.

Chapitre 2

Courbes Elliptiques de grand Rang

2.1 Introduction

Le calcul du rang d'une courbe elliptique ne cesse d'intriguer les théoriciens des nombres et jusqu'à aujourd'hui, il n'existe aucune formule calculatoire qui donne sa valeur exacte. La question de savoir s'il existe des courbes elliptiques de rang arbitraire a fait l'objet d'un large débat avec les conjectures initiales de Neron et Honda [21], une partie de spécialistes tels que Cassels [7], Tate [41], Mestre [26], Silverman [40] et Brumer [3] pense que le rang n'est pas borné. Mais suite à des études récentes [35], d'autres spécialistes comme (Park, Poonen, Voight et Wood) ont prédit qu'il est borné. Il est donc devenu intéressant de construire des courbes elliptiques avec des rangs exceptionnellement élevés. Dans ce qui suit, nous présentons quelques techniques qui permettent d'obtenir des courbes elliptiques de grand rang sur le corps des rationnels.

2.2 Méthode Basique

Beaucoup de familles de courbes (de grand rang) construites ont impliqués l'utilisation des mathématiques de haut niveau. Dans cette section, nous présentons une méthode très simple qui a permis à Dujella et Peral [15] d'obtenir une famille infinie de courbes elliptiques avec un sous groupe de torsion isomorphe à $\mathbb{Z}/8\mathbb{Z}$ et un rang supérieur ou égal à 2.
Pour une courbe d'équation

$$y^2 = x^3 + Ax^2 + Bx \qquad \text{où} \quad A, B \in \mathbb{Z}.$$

les coordonnées d'un point rationnel s'écrivent sous la forme :

$$x = \frac{du^2}{v^2} \qquad y = \frac{duw}{v^3}$$

où $d, u, v, w \in \mathbb{Z}$, d sans facteur carré et $\gcd(d, u) = \gcd(d, v) = \gcd(u, v) = 1$.
Par substitution des coordonnées du point dans l'équation de la courbe et après simplification on obtient

$$du^2w^2 = u^2(Bv^4 + d^2u^4 + Adu^2v^2)$$

ce qui implique que $d|B$. Ceci suggère fortement la recherche des points sur la courbe de la forme

$$x = \frac{d(t)u^2(t)}{v^2(t)}.$$

où $u(t)$ et $v(t)$ sont des simples polynômes et $d(t)$ est de la forme
$d(t) = \pm 2^e(t-1)^f(t+1)^g$. Autrement dit, on cherche un point avec la coordonnée x parmi les diviseurs de B ou un carré rationnel multiplié par les diviseurs de B.
Comme de nombreuses courbes avec cette torsion ont un rang 0, Il y a très peu de chance que nous trouvions un tel point directement. Nous pouvons néanmoins rechercher de tels points qui, lorsqu'ils sont substitués dans le membre à droit de la courbe, se simplifient à

$$(F(t))^2(at^2 + bt + c).$$

Nous aurons donc un point d'ordre infini (à l'exception d'un petit nombre de valeurs t) lorsque l'équation

$$(at^2 + bt + c) = \square$$

possède une solution. Dans ce cas là, nous essayons de paramétrer ces formes quadratiques. (Notez que nous n'avons pas toujours une forme quadratique possédant une solution).

Remarque 26. *La famille qui dérive possède le même sous groupe de torsion de la courbe du départ.*

Exemple 27. *Soit*

$$E_t : y^2 = x^3 - 9(8t^4 + 16t^3 + 8t^2 - 1)x^2 + (1296t^4(t+1)^4)x$$

C'est une courbe elliptique de rang générique 0 avec un sous groupe de torsion

isomorphe à $\mathbb{Z}/8\mathbb{Z}$ *généré par le point*

$$P = (36t^4 + 108t^3 + 108t^2 + 36t, 216t^5 + 756t^4 + 972t^3 + 540t^2 + 108t)$$

Pour augmenter le rang, nous avons trouvé deux possibilités :

1. *En prenant* $x = 6^2t^4$ *nous avons une forme quadratique* $16t^2 + 16t + 5$ *pour laquelle* $\frac{-k^2-4k+16}{2(k^2-16)}$ *est une paramétrisation.*
2. *La seconde est* $x = 6^2(t+1)^3(t-1)$*, donc un point rationnel se produit lorsque* $\frac{5t+3}{t-1} = \square$*. Cette équation est paramétrable dont* $t = \frac{w^2+3}{w^2-5}$ *est une solution.*

Dans les deux cas, on obtient une courbe elliptique sur $\mathbb{Q}(k)$ *(respectivement* $\mathbb{Q}(w)$*) de rang* ≥ 1*.*

2.3 Une Borne Inférieure

Les deux spécialistes David E. Penney et Carl Pomerance ont développé (dans [36]) une procédure pour déterminer une borne inférieur des courbes elliptiques de la forme

$$E : y^2 = x^3 + ax^2 + bx \tag{2.1}$$

où $(a, b) \in \mathbb{Z}$ et $a^2 - 4b$ n'est pas un carré.
Ce modèle de courbes possède un seul point d'ordre 2 a savoir $(0, 0)$. Donc, si Γ était son groupe de Mordell-Weil il s'écrira de la forme $\Gamma = \mathbb{Z}^r \times \mathbb{Z}_2$ où r désigne le rang de E, cela implique que

$$\Gamma/2\Gamma = (\mathbb{Z}_2)^{r+1}.$$

Notons aussi que, Si $P = (x, y) \in 2\Gamma$ alors $x \in \mathbb{Q}^2$.
Considérons maintenant l'application

$$\begin{array}{rcl} f : \Gamma & \longrightarrow & \mathbb{Q}^*/\mathbb{Q}^{*^2} \\ P & \longmapsto & f(P) = \left\{ \begin{array}{rl} f(x,y) & = x\mathbb{Q}^{*^2} \text{ si } x \neq 0, \\ f(0,0) & = b\mathbb{Q}^{*^2}, \\ f(O) & = \mathbb{Q}^{*^2}. \end{array} \right. \end{array}$$

f définit un homomorphisme tel que $2\Gamma \subset \ker f$.
Grâce à cet homomorphisme, il est possible d'obtenir des informations sur le rang de Γ. En effet, si l'on connaît l'image de f, on connaît aussi le groupe $\Gamma/2\Gamma$ dont le cardinal

est égal à 2^{r+1}, où r est précisément le rang de Γ. En particulier, nous avons l'inégalité suivante.

$$2^{r+1} \;=\; o(\mathbb{Z}_2^{r+1}) \;=\; o(\frac{\Gamma}{2\Gamma}) \;\geqq\; o(\frac{\Gamma}{\ker f}) \;=\; o(imf).$$

Par conséquent, si nous pouvions calculer $o(imf)$, nous aurions une borne inférieure pour le rang r de Γ.

Théorème 28 (Tate)**.** *$imf = \{b\mathbb{Q}^{*^2}\} \cup \{n\mathbb{Q}^{*^2} : n \in \mathbb{Z}, n|b$ et $nu^4 + \frac{bv^4}{n} + au^2v^2 = w^2$ a une solution (u, v, w) en nombres entiers non nuls premiers entre eux par paire $\}$.*

Démonstration. Confère [39]. □

Pour faciliter la résolution de la quartique mentionnée dans le Th.(28), nous limitons notre attention aux quartiques qui permettent une solution avec $u = v = 1$. Nous aurons alors affaire à l'ensemble

$$A = \{b\mathbb{Q}^{*^2}\} \cup \{n\mathbb{Q}^{*^2} : n \in \mathbb{Z}, n|b \text{ et } (n + \frac{b}{n} + a) \text{ est un carré}\}.$$

Si on désigne par B le sous groupe de imf engendré par les éléments de A, alors B est isomorphe à un sous groupe d'ordre $\mathbb{Z}_2^{r+1}$ c-à-d $o(B) = 2^s$ pour certain $s \leq r + 1$. Maintenant, il est claire que pour des valeurs a et b le calcul de $o(B)$ fournit une borne inférieure du rang de Γ.

Exemple 29. *On choisissons des valeurs pour a et b dans Eq.*(2.1)*, nous déterminons à l'aide d'un ordinateur le sous ensemble de A*

$$A' = \{n : n \in \mathbb{Z}, n|b \text{ et } (n + \frac{b}{n} + a) \text{ est un carré}\},$$

pour procéder au calcul de A puis $o(B)$.
Soit E la courbe elliptique déterminée par les valeurs $a = 167$ et $b = -210$

$$E : y^2 = x^3 + 167x^2 - 210x$$

<u>*Calcul des diviseurs de 210 :*</u>
$Div(210) =$
$\{\pm1, \pm2, \pm3, \pm5, \pm6, \pm7, \pm10, \pm14, \pm15, \pm21, \pm30, \pm35, \pm42, \pm70, \pm105, \pm210\}$
<u>*Calcul de A' :*</u>

$$A' = \{-6, -30, -70, -105, 2, 3, 7, 35\},$$

Cela implique que $o(B) = 8 = 2^3$ $(s = 3)$.
D'où la borne inférieur du rang

$$r \geq s - 1 = 2.$$

2.4 Méthode de Mestre (Polynômiale)

Mestre à développé une méthode très ingénieuse qui diffère de toute autre méthode de recherche de courbes elliptiques de haut rang car elle est la seule qui permet de construire des courbes elliptiques sur $\mathbb{Q}(t)$ à partir d'un nombre de points donnés. Nous allons la décrire puis l'illustrer par un exemple numérique.
l'idée repose sur le lemme suivant dont la démonstration se trouve dans [27].

Lemme 30. *Soient k un corps de caractéristique différente de 3, et $p(X)$ un polynôme unitaire de degré 12 à coefficients dans k. Il existe alors un unique triplet (g, r_1, r_2) d'éléments de $k[X]$ tels que :*

1. *g est unitaire de degré 4,* $\deg(r_1) \leq 3$ *et* $\deg(r_2) \leq 3$.
2. $p = g^3 + r_1 g + r_2$.

Si on note C la courbe d'équation $p = y^3 + r_1(x)y + r_2(x) = 0$ alors elle contient les points $P_i = (x_i, g(x_i))$ où les x_i parcours les racine de p. Mestre à prouvé que si $k = \mathbb{Q}(t)$ alors :

1. Le degré de $r_1 \leq 2$.
2. C est une cubique non singulière sur k d'invariant modulaire non constant.
3. Les points $P_i, i = l, ..., 12$ sont linéairement indépendants dans $Pic(C)$.
4. Les racines de p appartiennent à k.

En choisissant par exemple le point P_{12} comme origine, on obtient une courbe elliptique sur k dont le groupe de Mordell-Weil est de rang 11 sur $\mathbb{Q}(t)$. Si d'avantage les racines de $p(X)$ vérifient certaines conditions, Mestre ([26]) à démontrer que la la courbe elliptique C possède un point additionnel indépendant des autres racine de $p(X)$ ce qui donne une courbe elliptique de rang ≥ 12 sur le corps de fonction $\mathbb{Q}(t)$.
Suivant l'approche de Mestre, (Nagao [30], Fermigier[17] et Dujella [10]) ont obtenu des courbes elliptiques possédant un sous groupe de torsion non trivial et un rang particulièrement élevé.

Exemple 31. *Pour tout* $(a_1, a_2, ..., a_n) \in \mathbb{A}^n(\mathbb{Q}(t))$ *soit*

$$p(X) = (X^2 - a_1^2)(X^2 - a_2^2) \cdots (X^2 - a_n^2) \in \mathbb{Q}(t)[X].$$

Selon la méthode de Mestre (légèrement modifiée par Fermigier) nous pouvons écrire le polynôme $p(X)$ sous la forme

$$g(X)^2 - r(X)$$

où $\deg g(X) = n$ *et* $\deg r(X) \leq n-1$.
Considérons la courbe

$$C : Y^2 = r(X).$$

Si on arrive a bien choisir les a_i de sorte que C définit une courbe elliptique (Cubique ou quartique) alors, la courbe C possèdera les points $(\pm(a_i), g(\pm a_i))$ pour $i = 1, .., n$.
Pour $n = 8$ et $A = (a_1, a_2, ..., a_8)$ où les $a_i \in \mathbb{Q}$. Fermigier a établi la condition suivante pour que $\deg r = 4$.

Condition 32. $a_1^2 + a_2^2 = a_3^2 + a_4^2 = a_5^2 + a_6^2 = a_7^2 + a_8^2 = s$.

Prenons $s = p_1p_2p_3$ où les p_i $(i = 1, 2, 3)$ sont des nombres premiers distincts congrus à 1 modulo 4. Chaque p_i s'écrit donc comme somme de deux carrés, ainsi le produit "s" s'écrira comme somme de deux carrés en 4 manières différentes.
Andrej Dujella dans [10] a donné une formule explicite de ces quatre écritures de s en fonction des écritures des p_i en somme de deux carrés. Si $p_1 = a^2 + b^2$, $p_2 = c^2 + d^2$ et $p_3 = e^2 + f^2$ alors

$$p_1p_2p_3 = x_1^2 + x_2^2 = x_3^2 + x_4^2 = x_5^2 + x_6^2 = x_7^2 + x_8^2$$

où

$$\begin{aligned}
x_1 &= e(ac + bd) + f(ad - bc) \\
x_2 &= f(ac + bd) - e(ad - bc) \\
x_3 &= e(ac + bd) - f(ad - bc) \\
x_4 &= f(ac + bd) + e(ad - bc) \\
x_5 &= e(ac - bd) + f(ad + bc) \\
x_6 &= f(ac - bd) - e(ad + bc) \\
x_7 &= e(ac - bd) - f(ad + bc) \\
x_8 &= f(ac - bd) + e(ad + bc)
\end{aligned}$$

Si on pose $p_1 = 5$, $p_2 = 53$, $p_3 = 881$ ($p_i \equiv 1\,[4]$), alors on a

$$p_1 = 1^2 + 2^2,\ p_2 = 7^2 + 2^2,\ p_3 = 16^2 + 25^2$$

et $s = 5 \times 53 \times 881 = 233\,465$ *qu'on peut l'écrire comme :*

$$s = 83^2 + 476^2 = 124^2 + 467^2 = 181^2 + 448^2 = 331^2 + 352^2$$

Soit maintenant $p(x) = \prod_{i=1}^{8}(x - x_i)$ *,* $q(x) = p(x)p(-x) = g(x)^2 - r(x)$.
Calcul des polynômes : p, q, g et r

$$\begin{aligned} p(x) &= (x-83)(x-476)(x-124)(x-467)(x-181)(x-448)(x-331)(x-352) \\ &= x^8 - 2462x^7 + 2563\,792x^6 - 1466\,930\,922x^5 + 501\,119\,203\,215x^4 \\ &\quad -103\,857\,097\,595\,688x^3 + 12\,645\,957\,007\,876\,208x^2 - 820\,798\,401\,894\,972\,928x \\ &\quad +21\,614\,781\,861\,342\,838\,784 \end{aligned}$$

$$\begin{aligned} q(x) &= p(x) \times p(-x) \\ &= (-x-83)(-x-476)(-x-124)(-x-467)(-x-181)(-x-448) \\ &\quad (-x-331)(-x-352)(x-83)(x-476)(x-124)(x-467)(x-181) \\ &\quad (x-448)(x-331)(x-352) \\ &= (x-83)(x+83)(x-124)(x+124)(x-181)(x+181)(x-331)(x+331) \\ &\quad (x-352)(x+352)(x-448)(x+448)(x-467)(x+467)(x-476)(x+476) \\ &= x^{16} - 933\,860x^{14} + 352\,099\,965\,766x^{12} - 68\,455\,955\,967\,202\,820x^{10} \\ &\quad +7262\,905\,017\,329\,061\,309\,121x^8 - 409\,310\,424\,944\,247\,095\,893\,717\,280x^6 \\ &\quad +11\,091\,913\,709\,115\,800\,159\,549\,912\,371\,456x^4 \\ &\quad -127\,030\,812\,247\,013\,459\,612\,433\,506\,706\,391\,040x^2 \\ &\quad +467\,198\,794\,913\,435\,394\,380\,418\,532\,479\,814\,598\,656 \end{aligned}$$

Pour satisfaire l'égalité $q(x) = g(x)^2 - r(x)$ *on pose* $g = x^8 + ax^6 + bx^4 + cx^2 + d$*, donc*

$$\begin{aligned} g^2(x) &= \left(x^8 + ax^6 + bx^4 + cx^2 + d\right)^2 \\ &= x^{16} + 2ax^{14} + x^{12}\left(a^2 + 2b\right) + x^{10}(2c + 2ab) + x^8\left(b^2 + 2d + 2ac\right) \\ &\quad +x^6(2ad + 2bc) + x^4\left(c^2 + 2bd\right) + 2cdx^2 + d^2 \end{aligned}$$

les monômes dans $g^2(x)$ *de degré respectivement* $14, 12, 10, 8$ *et* 6 *doivent avoir les mêmes coefficients que les monômes dans* $q(x)$ *de degré respectivement* $14, 12, 10, 8$ *et* 6.

Donc on abouti au système

$$\begin{cases} 2a = -933\,860 \\ a^2 + 2b = 352\,099\,965\,766 \\ 2c + 2ab = -68\,455\,955\,967\,202\,820 \\ b^2 + 2d + 2ac = 7262\,905\,017\,329\,061\,309\,121 \\ 2ad + 2bc = -409\,310\,424\,944\,247\,095\,893\,717\,280 \end{cases}$$

dont la solution est :

$$\begin{aligned} a &= -466\,930, \\ b &= 67\,038\,170\,433, \\ c &= -2925\,845\,063\,320\,720, \\ d &= 18\,229\,525\,746\,209\,161\,216. \end{aligned}$$

d'où les polynômes

$$\begin{aligned} g(x) &= x^8 - 466\,930x^6 + 67\,038\,170\,433x^4 - 2925\,845\,063\,320\,720x^2 \\ &\quad +18\,229\,525\,746\,209\,161\,216. \end{aligned}$$

et

$$\begin{aligned} r(x) &= g^2(x) - q(x) \\ &= -87\,196\,266\,783\,309\,626\,707\,968\,000\,000x^4 \\ &\quad +20\,357\,276\,424\,565\,381\,999\,375\,749\,120\,000\,000x^2 \\ &\quad -134\,883\,185\,981\,732\,718\,320\,101\,449\,793\,536\,000\,000 \end{aligned}$$

En utilisant le logiciel Magma [2] (Computational Algebra System) on peut récolter tous les informations sur la courbe elliptique $y^2 = r(x)$.
Le corps de définition $Q(x)$:
$Q < x >$:=PolynomialRing(Rationals()) ;
Definir le polynôme $r(x)$:
*> r :=-87196266783309626707968000000*x^4 +*
*20357276424565381999375749120000000*x^2-*
13488318598173271832010144979353600000 0 ;
> E :=AssociatedEllipticCurve(r) ;

> E ;
Elliptic Curve defined by $y^2 + x * y =$
$x^3 - 12145646525480873356099625 * x - 22766402964550664137743885731186691 9$ *over Rational Field*
> TorsionSubgroup(E) ;
Abelian Group isomorphic to $Z/2$ *Defined on 1 generator.*
Pour le calcul du rang et des générateurs de E on utilise la commande (DescentInformation(E) ;) qui utilise la 2-descente et d'autre techniques pour calculer le rang de E est les générateurs y compris ceux du sous groupe de torsion ainsi que des informations sur le groupe de Selmer et celui de Tate-Shafarevich. >
SetClassGroupBounds("GRH") ;
> DescentInformation(E) ;
Torsion Subgroup = Z/2
The 2-Selmer group has rank 12
Found a point of infinite order.
Found 2 independent points.
Found 3 independent points.
Found 4 independent points.
Found 5 independent points.
Found 6 independent points.
Found 7 independent points.
Found 8 independent points.
Found 9 independent points.
Found 10 independent points.
Found 11 independent points.
After 2-descent :
11 <= Rank(E) <= 11
Sha(E)[2] is trivial
(Searched up to height 100 on the 2-coverings.)
$[11, 11]$
Cette courbe est de rang égal à 11 et voici un exemple de 11 points indépendants donnés par leur abscisses :
$x(P_1) = (846123751950146596/223729)$
$x(P_2) = (-16256409987287785208206933 4/1494805995123841)$
$x(p_3) = (-6341093468618286809259555293725932 6/48874182747811212963649)$
$x(p_4) = (-50434519532492595034790/18776398729)$

$x(p_5) = (8468722874842858352 2/14070001)$
$x(p_6) = (690648475216528707400498501299690/120077731367078217121)$
$x(p_7) = (955442889111931043771586090 34/5803630541122969)$
$x(p_8) = (-219462289198847620066913497598/63998819178854641)$
$x(p_9) = (-34942395231235239374/24235929)$
$x(p_{10}) = (9558164759403837874/25281)$
$x(p_{11}) = (-120378561327509559254/141871921)$.

2.5 Méthode du corps fini

La méthode de calcul que nous allons présenter ici, permet à partir d'une courbe elliptique sur un corps de fonctions rationnels d'isoler les courbes elliptiques qui ont plus de chance d'avoir un rang élevé. Les spécialistes pensent qu'une courbe elliptique définie sur $\mathbb{Q}$ est de rang élevé si elle admet beaucoup de points sur les corps fini $\mathbb{F}_p$, $p \leq N$ (pour N assez grand). Mestre à développé une formule calculatoire qui compte les points d'une courbe elliptique sur plusieurs corps fini et donne une sorte de moyenne avec laquelle on peut juger la courbe bonne ou pas, depuis, cette formule à été adaptée par Nagao [32, 33].

la somme de Mestre-Nagao :
Pour une courbe elliptique E sur le corps des rationnels et un nombre premier p, on pose $a_p = p + 1 - |E(\mathbb{F}_p)|$. Pour un entier N fixe, la somme de Mestre-Nagao d'une courbe elliptique E est définie par

$$S(N, E) = \sum_{p \leq N : p \text{ premier}} \left(1 - \frac{p-1}{|E(\mathbb{F}_p)|}\right) \log p = \sum_{p \leq N : p \text{ premier}} \frac{-a_p + 2}{p + 1 - a_p} \log p. \tag{2.2}$$

Il est expérimentalement connu [26, 30, 31] et fortement soutenu par la conjecture BSD (voir [5]) que nous pouvons nous attendre à trouver des courbes de haut rang en regardant celles qui ont un grand $S(N, E)$. Cette méthode a été exploitée dans diverses constructions [1, 10, 14, 30, 31] avec succès.

Exemple 33. *Soit la courbe elliptique donnée par l'équation :*

$$E_{(a,b,c)} : y^2 = x^3 + b^2x^2 - c^2x + a^2 \tag{2.3}$$

tel que (a, b, c) forme un triplet de Pythagore (c-à-d : $a^2 + b^2 = c^2$). En utilisant la paramétrisation

$$a = t^2 - 1 \qquad b = 2t \qquad c = t^2 + 1. \tag{2.4}$$

La courbe $E_{(a,b,c)}$ se réduit à :

$$E_t : y^2 = x^3 + (2t)^2x^2 - (t^2+1)^2x + (t^2-1)^2 \tag{2.5}$$

Maintenant, nous essayons de trouver des courbes elliptiques dans cette famille avec un grand rang en calculant $S(10^6, E_t)$ avec Pari-Gp [34] puis choisissons les meilleurs candidats.
Pour $2 \leq t \leq 250$ les résultats son listés dans le tableau suivant :

TABLE 2.1 – Somme de Mestre-Nagao

t	$S(10^6, E_t)$
2	35.041941748370927702067381 65
3	44.414902037311273894874991 79
4	45.733399137386392746717156 18
5	47.388599312519087741121434 47
6	61.301366252656287409715202 78
7	62.254889476136722608310636 70
8	69.117177309433675132154810 69
9	52.295850993168275753728473 78
10	34.326948224985593800653780 47
11	29.892554583557029077690521 29
12	44.484821190983882320262204 46
13	73.862281040389574412521754 31
14	68.972590989864364703678182 58
15	46.317262952428618041361836 30
16	29.335134879562357954073727 40
17	41.932788928000937689370041 47
18	35.818973495258189753450356 66
19	59.031534908916219849372589 89
20	29.700040851829438169940543 78
21	60.207877266866001222658901 79
22	25.088683456367437400102013 77
23	57.951021513395641382022866 90
24	39.276944844168071729679302 50
25	39.528541795264726640648909 57
26	41.455320858056604756054526 39
27	72.532890633838215523792118 88
28	47.433959845331948589571468 96
29	45.899264272741209403403431 91
30	53.293880267681911245320926 32
31	49.516973709044048483832992 99
32	33.620846525608649592891204 07

t	$S(10^6, E_t)$
33	34.59332956451323949293007634
34	68.47624422767416176806795304
35	50.68586804126722120197715726
36	64.69926613630382086089945160
37	42.63282905881404217612255062
38	43.47381398167948922327015990
39	44.00373004085534394751779616
40	49.69137623405797455744595161
41	52.00160093414589539853187333
42	88.74307683919607624769135591
43	38.63335608404479922315703048
44	49.87365502042947705108212448
45	61.28668067415707202272300637
46	49.07888111414507943726705235
47	45.65056970017921963475899480
48	18.11919023262765880307737938
49	61.85370224378875720715964132
50	41.33804170970543687914937903
51	40.66055030935739679217614856
52	39.45568964359857858023022167
53	41.94738552726051793579241694
54	36.89971189416643016171820674
55	45.77524765830173481679956908
56	26.82624799881187360757178099
57	41.59958110649729230410536090
58	46.00104794775096115428674362
59	34.85287527800202730493374357
60	49.04840954850435432686468553
61	37.00366595197358535108515090
62	46.52108705950390459771411124
63	50.78248123795839517814417327
64	43.91426199596713194723748193
65	60.31070366799670117629499855
66	51.13999310294950600434945903
67	47.29460173240954458039255618
68	52.11521513613074401404297651
69	48.24557006094896008982430692
70	35.30815662136671972464620107
71	54.22186633602326182241133597
72	40.27736447810346675467689318
73	55.00327814415458723450126691
74	49.29082304969763090537710997

t	$S(10^6, E_t)$
75	44.52009582871829602937834163
76	45.65413216325246168320618094
77	57.02604928394608274932853833
78	47.48208484360729019141647651
79	60.93662109252180640567480465
80	42.29002679109008167082127669
81	48.19173821013421581342993743
82	41.50941108920106818463387765
83	33.91163257906023754030782007
84	34.33534611340464477156538294
85	33.80663567921127030396746725
86	47.06980942935673259366556665
87	55.08581822552546161455131561
88	38.48358817817360975584150903
89	39.41224630143087414493967560
90	43.29184371091534432121227546
91	35.72998220135023717714566673
92	50.51353985961278464140909253
93	40.70244383067250791957705161
94	53.33496127173337230789121170
95	69.00915609318776635695356762
96	39.21295104261485633151188477
97	44.50267919694195256264487282
98	57.80835002279918855208842043
99	39.10832866711182989076035880
100	44.52757529524403540688208682
101	54.44959336935919972434679114
102	26.00458786166629868710548983
103	37.32352440648248079518837152
104	58.99063030359743518868041709
105	44.12730773911384254537506583
106	48.51378589447555593066857772
107	41.27423993166424970474060893
108	60.97768497157184352221157608
109	48.07502691405155812379663012
110	58.29907878856110956960742040
111	45.29421527701891367358887819
112	61.26881244141945183427484948
113	45.24072748453773161387762546
114	41.87270942545292476096771265
115	41.73128063121100791894538167
116	39.61278390704742861089470211
117	47.09997192877745782839591227

t	$S(10^6, E_t)$
118	45.59852477505414599451798910
119	49.38791979286404367390412163
120	47.95201727168133165150868078
121	43.31671962808881276823119014
122	55.59540652923159549287317071
123	52.56830665582721903776822265
124	32.97690012075336734241274106
125	58.94729766643180801718746559
126	37.09044757966687614281759977
127	47.57165931649099213074343515
128	39.70094659263926090460061013
129	43.78170966336104870484464051
130	38.99652748469595947288173431
131	44.94290961520757973344524161
132	48.83444033000968078080628013
133	28.50980320829311200824445453
134	41.35727698259525773986107258
135	40.77549606328852674832771614
136	50.60905481643409586770952701
137	55.04183944907421902997286069
138	50.92371568963123721717606926
139	32.58691296440982889202903180
140	37.23721981769136500760158755
141	36.04035096356112089049281445
142	47.93807610733675856432058647
143	31.41287752101196921490918014
144	42.29512382801315966330123167
145	49.76525862757707351383711640
146	48.13599526473039146868676680
147	56.32167221809078849473552664
148	47.04876347179187908429834186
149	34.96031492991318762910022492
150	31.09447545998770186636193827
151	43.86474149824407410577992017
152	39.11908282344129976081597599
153	43.85668384034872567319198685
154	46.12250105576952774830744953
155	38.52403500786777272355632791
156	72.23420838190368007626532195
157	43.61162871826247134948592795
158	34.57532382003274193511593808
159	40.71273020764739404026845786

t	$S(10^6, E_t)$
160	64.604970372275323770475045 58
161	38.977120084035537709987205 96
162	53.028237343871434113482917 32
163	29.478555757365981533747254 56
164	52.907613649470434605437872 93
165	74.326316339739152714717367 09
166	24.427605240034993753507231 97
167	44.162683245327123083313004 16
168	64.330693526800585943001653 38
169	34.367452596635653174927109 11
170	49.450109298230921604160652 19
171	39.820380553651593206296759 35
172	38.217285361750544532590815 11
173	50.041349657646782625618482 57
174	49.157746732753769358872795 33
175	32.244568485172843365652355 47
176	51.858635927161816067927359 50
177	44.683142238895793902883824 72
178	50.000747737094070218965906 32
179	39.986103413127916720022513 75
180	51.959857602807454265705831 31
181	43.842112162831286001694073 58
182	48.334214486095272342418392 23
183	40.892292789481086071306077 64
184	40.362537227292916973932774 64
185	50.715839925473188391818851 20
186	41.102588477854308322476350 49
187	52.820055817883337401712137 39
188	44.636867822709333824838313 74
189	67.084999903123368310425821 63
190	55.285078927674905564594407 07
191	52.994717628890584708163906 24
192	48.239806847908139854445102 16
193	37.757525108948496402324560 54
194	48.959410567647040432025651 39
195	59.105328721640801905487772 17
196	61.300075393699357954189609 31
197	66.729055120823640423788887 33
198	31.386965400331376181709753 44
199	49.354011813809238535602792 02
200	54.181203537711454971819866 41

t	$S(10^6, E_t)$
201	54.233896894400226526367973 11
202	41.365115545183758523341338 99
203	44.313407603165398571336109 87
204	42.504857915626038564930578 08
205	51.170569679930490216255795 30
206	49.489808201251707711746616 93
207	46.910981557776251575306509 03
208	40.896992407484262733643103 26
209	55.974758932723781901406343 18
210	38.999904917633353397673147 48
211	29.786948698501389497589959 61
212	49.943227108836424519307568 34
213	40.352606853948877822904663 17
214	54.949562368623056766125674 44
215	55.042190414325290965437739 66
216	43.802383166820103253376308 38
217	64.552989104548126020573843 65
218	58.352149479610599271202483 40
219	54.787429143676628182358161 22
220	59.233899011019776375195971 59
221	47.310040007728160478068061 47
222	35.443324059673429620132144 65
223	86.572618272290356622746600 40
224	44.547066863706658861266188 76
225	46.490332002248897626532579 05
226	38.890356238699397535114167 40
227	48.233373676497405991324904 66
228	63.698398045445318329103254 62
229	40.471700856087059103900496 12
230	61.270147849462220835213013 96
231	42.636643716702120342716255 61
232	45.416086604072270332406276 52
233	46.310630421859012473292861 47
234	54.334969799033114381334020 36
235	41.725558686082485559846022 73
236	47.791733937602173390708137 08
237	40.796143229935857367390571 25
238	41.173248399296708625804651 26
239	48.248397315248335113541385 39
240	42.722405143232022764370596 09
241	43.644418209705106237470253 72
242	49.349724643045378887724108 22

t	$S(10^6, E_t)$
243	42.38887226741160909127501488
244	79.84715664292854792621607727
245	54.39059995174328483427736401
246	50.40160669824932066081032904
247	25.74010608602038245257612684
248	51.04920435035549200403589044
249	31.84649923836776158255929929
250	46.28044373710566026374603672

Pour $t = 223$*, nous avons une grande valeur*

$$S(10^6, E_{223}) = 86.57261827229035662274660040.$$

Nous allons voir que la courbe

$$E_{223} : y^2 = x^3 + 198916x^2 - 2473072900x + 2472873984$$

possède vraiment un rang élevé.
Il est difficile de calculer le rang exact de E_{223}*, mais on peut tout de même montrer qu'elle a un rang supérieur ou égal à 8. Pour cela, il suffit de chercher dans cette courbe suffisamment de points entiers pour générer un sous-groupe de rang 8. Comme suggéré,* ($r \geq 8$) *le calcul des points entiers révèle* 28 *paires* (x, y) *avec* $x < 10^8$ *et voici un exemple de 8 points entiers indépendants*

$$\begin{aligned}
p_1 &= (-210626, 1183868),\\
p_2 &= (-210064, -5251624),\\
p_3 &= (-209671, -6761923),\\
p_4 &= (-206658, 13432836),\\
p_5 &= (-205888, 14616304),\\
p_6 &= (-201870, 19464372),\\
p_7 &= (-50174, -22327876),\\
p_8 &= (-34670, 16827628).
\end{aligned}$$

Mais, tous (les 28 points entiers) dans le même groupe de rang 8. Pour déterminer son rang exact, nous avons envoyé le modèle minimal de la courbe E_{223} *au forum MathOverFlow, 15 minutes plus tard, le fameux spécialiste N. Elkies à pris le challenge*

de calculer les générateurs de cette courbe. Donc, un grand merci à N. Elkies pour son aide et pour le temps qu'il a consacré au calcul des générateurs de la courbe elliptique E_{223} en utilisant le calculateur de germain. math. Harvard et appliquant le programme "mwrank" de John Cremona [8] sur cette courbe où il a été surpris par le temps qu'il a fallu (3 semaines !) pour calculer les générateurs d'une courbe avec des coefficients de cette taille !.
Le fait que "mwrank" ait pu le faire en trois semaines pourrait encore être un point intéressant sur ce type de calcul.
Puis, il nous a communiqué les générateurs du modèle minimal correspondant à E_{223} que nous donnons par leur coordonnée x :

$$\begin{aligned}
x_1 &= (78271)\\
x_2 &= (78077)\\
x_3 &= (10092319809/2197)\\
x_4 &= (4284948894/54872)\\
x_5 &= (6394749009/35937)\\
x_6 &= (8109376287/103823)\\
x_7 &= (5638548716266233736152/98759759636551168)\\
x_8 &= (73421481/343)
\end{aligned}$$

Remarque 34. *Cela confirme que E_{223} est de rang exactement 8.*

Chapitre 3

Courbe elliptique de rang au moins 5 et suite arithmétique de langueur 7

Soit $E_{a,b} : y^2 = x^3 + a^2x^2 - (a^2 + b^2)x + b^2$ une courbe elliptique définit sur le corps de fonctions $\mathbb{Q}(a, b)$. Dans ce qui suit, nous construisons une sous famille de $E_{a,b}$ ayant au moins 5 points $\mathbb{Q}(t, k)$-rationnels indépendants. Ensuite, en utilisant les points à coordonnées entières et avec des méthodes élémentaires nous donnerons une sous famille de $E_{a,b}$ ayant une infinité de courbes elliptiques possédants 7 points dont les cordonnées en "x" forment une suite arithmétique de longueur 7.

3.1 Structure de la courbe Elliptique $E_{a,b}$

Soit $E_{a,b}$ la courbe elliptique sur le corps de fonctions $\mathbb{Q}(a, b)$ donnée par l'équation de Weierstrass

$$E_{a,b} : y^2 = x^3 + a^2x^2 - (a^2 + b^2)x + b^2. \tag{3.1}$$

Le discriminant D de $f(x)$ (second membre de (3.1)) est égal à

$$D = 16a^8 - 32a^6b^2 + 64a^6 + 16a^4b^4 - 96a^4b^2 - 96a^2b^4 + 64b^6 - 432b^4. \text{(Non Constant)} \tag{3.2}$$

On rappelle qu'un point $P = (x, y)$ sur E est dit entier (ou intégral), si ses coordonnées sont dans $\mathbb{Z}$, le point à l'infini O est considéré comme tel ; tout comme les points d'ordre fini, ils ont toujours des coordonnées dans $\mathbb{Z}$, ce fameux résultat a été prouvé par Nagell-Lutz (voir la preuve complète dans [39], corolaire 7.2), mais ce n'est guère une déclaration -si et seulement si- ce qui laisse la possibilité à d'autres points entiers d'y être, ces derniers seront d'ordre infini.
Dans $E_{a,b}$ on peut trouver facilement au moins deux points entiers, à savoir $P_0 = (0, b)$

et $P_1 = (1, 1)$. Nous verrons par la suite que $E_{a,b}$ possède aussi d'autre points à coordonnées entières.
Notons que le sous-groupe de torsion de l'Eq(3.1) n'est pas toujours trivial, pour certaines valeurs de a et b nous avons un point de torsion comme nous pouvons le voir dans ce qui suit

Proposition 35. *Soient $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $E_{a,b}$ une courbe elliptique d'équation*

$$y^2 = x^3 + a^2x^2 - (a^2 + b^2)x + b^2,$$

alors :
Pour $a = b$ nous avons $E_{(a,b)_{Torsion}} \simeq \frac{\mathbb{Z}}{3\mathbb{Z}}$.

La courbe elliptique E_a peut s'écrire de la forme

$$E_a : y^2 = x^3 + (ax - a)^2$$

qui est un cas particulier de la courbe étudiée par S. Kihara dans [24] de la forme $y^2 = ax^3 + (bx - c)^2$. Son sous groupe de torsion est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ engendré par le point $(0, a)$. Top [43] a également montré que certaines courbes de ce type ont le rang 3 sur $\mathbb{Q}$. de même, G. Campbell [5] a construit à partir de ce type de courbes une courbe elliptique de rang au moins 3 sur $\mathbb{Q}(t)$.
La courbe elliptique $E_{a,b}$ contient aussi les points entiers d'abscisses

$$\begin{aligned} x(P_2) &= \quad a + b, \\ x(P_3) &= \quad a - b, \\ x(P_4) &= -a + b, \\ x(P_5) &= -a - b, \end{aligned} \tag{3.3}$$

et par addition nous avons aussi

$$\begin{aligned} P_6 = P_0 + P_1 &= (-a^2 + b^2 - 2b, -a^2b + a^2 + b^3 - 3b^2 + b), \\ P_7 = P_3 + P_5 &= (-a^2 + b^2 + 2b, a^2b + a^2 - b^3 - 3b^2 - b). \end{aligned}$$

Fasciné par le nombre de points entiers sur cette courbe (sans oublier les symétriques), nous avons effectué un test pour calculer le rang de $E_{a,b}$ en utilisant Magma [2], et après tout ce que nous avons recueilli lors des expérimentations, nous étions en mesure de

prédire une autre particularité de $E_{a,b}$, il semble que pour certaines conditions sur a et b le rang est toujours supérieur ou égal à 3 et parfois beaucoup plus élevé. Ainsi, nous pouvons alors prouver le théorème suivant.

Théorème 36. *Pour $a \neq b$ et $a \pm b \neq \pm 1$ il existe une infinité de courbes elliptiques $E_{a,b}$ avec un groupe de Mordell-Weil de rang ≥ 3.*

Ces conditions découlent du fait que si $a = b$ alors, P_0, P_3 et P_4 représentent le même point. De même, lorsque $a - b = \pm 1$ d'autres points coïncident avec P_1 ce qui en général diminue le rang de la courbe. Pour calculer une borne inférieure du rang qui est suggéré comme étant ≥ 3, nous utilisons le théorème de spécialisation de Silverman [38], il indique que si un ensemble de n points $\mathbb{Q}(a,b)$-rationnels d'une courbe elliptique $E_{a,b}$ sur $\mathbb{Q}(a,b)$ sont indépendants par spécialisation à une seule valeur $(a,b) \in \mathbb{Q} \times \mathbb{Q}$, alors ils restent ainsi pour tous sauf un nombre fini de (a,b). Il suffit donc de montrer que l'ensemble des points intégral engendre un sous-groupe de rang 3 pour une valeur unique de (a,b).

Démonstration. Par spécialisation à $(a,b) = (5,11)$, nous obtenons la courbe

$$E_{5,11} : y^2 = x^3 + 25x^2 - 146x + 121.$$

Les trois points P_0, P_1 and P_2 qui correspondent dans la courbe résultante à

$$P_0 = (0,11), P_1 = (1,1) \text{ et } P_2\,(16,91)$$

ont un régulateur non nul $\approx 5.943317267936188733333741373572 \neq 0$ tel que calculé par Magma, montrant que ces trois points sont indépendants et donc $E_{5,11}$ a le rang ≥ 3. Le résultat de la spécialisation de Silverman implique que pour tous sauf un nombre fini de couples rationnels (a,b), le rang de $E_{a,b} \geq 3$. □

3.2 Sous Famille de Rang au moins 5

Afin d'augmenter le rang de 2, nous imposons sur la courbe deux points supplémentaires Q_1 et Q_2 de coordonnées $x\,(Q_1) = -a^2$ et $x\,(Q_2) = \dfrac{b^2}{a^2+b^2}$ sur $E_{a,b}$, de sorte que P_0, P_1, P_2, Q_1 et Q_2 soient indépendants. Pour cela, nous devons résoudre le système suivant

$$S = \begin{cases} a^2b^2 + a^4 + b^2 = \square, \\ a^2 + b^2 = \square. \end{cases} \tag{3.4}$$

La première équation possède la solution paramétrée

$$b = \frac{2a^2h}{a^2 - h^2 + 1}.$$

En remplaçant b dans la deuxième équation, nous avons :

$$\begin{aligned} a^2 + b^2 = & \quad a^2 + \left(\frac{2a^2h}{a^2 - h^2 + 1}\right)^2, \\ = & \quad a^2 \frac{(-2h + a^2 + h^2 + 1)(2h + a^2 + h^2 + 1)}{(a^2 - h^2 + 1)^2}, \\ = & \quad a^2 \frac{(a^2 + (h-1)^2)(a^2 + (h+1)^2)}{(a^2 - h^2 + 1)^2}. \end{aligned} \tag{3.5}$$

Maintenant, nous devons juste faire de $(a^2 + (h-1)^2)$ et $(a^2 + (h+1)^2)$ des carrés rationnels parfaits.
En effet, Sur $\mathbb{Q}(h)$ la conique $(a^2 + (h-1)^2) = A^2$ possède la solution
$(a, A) = (0, (h-1))$, donc une solution paramétrique peut être donnée par

$$a = \frac{(2t - 2th)}{(t^2 - 1)}.$$

De même, après avoir remplacé la valeur de $a = \dfrac{(2t - 2e)}{(t^2 - 1)}$ dans le deuxième terme $(a^2 + (h+1)^2)$, nous devons vérifier la résolubilité de l'équation

$$(t^4 + 2t^2 + 1)h^2 + (2t^4 - 12t^2 + 2)h + (t^2 + 1)^2 = B^2.$$

Sur $\mathbb{Q}(t)$ cette dernière possède la solution $(h, B) = (0, (t^2 + 1))$, donc une solution paramétrique peut être donnée par

$$h = \frac{2k + 2kt^2 + 12t^2 - 2t^4 - 2}{-k^2 + 2t^2 + t^4 + 1}.$$

En termes de t et k, la courbe elliptique $E_{a,b}$ devient

$$E_{t,k} : y^2 = x^3 + (a(t,k))^2 x^2 - ((a(t,k))^2 + (b(t,k))^2)x + (b(t,k))^2$$

où

$$\begin{aligned} a(t,k) = & \quad \tfrac{2t(k+3t^2-1)(k-t^2+3)}{(t-1)(t+1)(k+t^2+1)(k-t^2-1)}, \\ b(t,k) = & \quad \tfrac{-16t^2(k-t^2+3)(k+3t^2-1)(k+kt^2+6t^2-t^4-1)}{(k+t^2+1)(k+4t+kt^2+6t^2-4t^3-t^4-1)(k-4t+kt^2+6t^2+4t^3-t^4-1)(k-t^2-1)}, \end{aligned}$$

et contient les points $\mathbb{Q}(t,k)$-rational d'abscisses

$$\begin{aligned} P_0 &= 0, \\ P_1 &= 1, \\ P_2 &= a(t,k)+b(t,k), \\ Q_1 &= -(a(t,k))^2, \\ Q_2 &= \frac{(b(t,k))^2}{(a(t,k))^2+(b(t,k))^2}. \end{aligned} \tag{3.6}$$

Enfin, nous pouvons affirmer ce qui suit

Théorème 37. *La courbe elliptique $E_{a,b}$ possède une sous famille $E_{t,k}$ de rang au moins 5 sur $\mathbb{Q}(t,k)$.*

Démonstration. Par Spécialisation à $(t,k)=(5,11)$ on obtient la courbe elliptique d'équation

$$E_{5,11}: y^2 = x^3 + \frac{874225}{1774224}x^2 - \frac{6208942650625}{6698137381776}x + \frac{20198094400}{46514842929},$$

et les points P_0, P_1, P_2, Q_1 et Q_2 de (3.6) correspondent à

$$\begin{aligned} P_0 &= (0, 142120/215673), \\ P_1 &= (1,1), \\ P_2 &= (111265/2588076, 2167613305/3447317232), \\ Q_1 &= (-874225/1774224, 3253980455/3447317232), \\ Q_2 &= (3326976/7102225, 321625516288/700314896125). \end{aligned}$$

Leur régulateur est non nul et égal à 380202.439920539902301420249295 tel que calculé par Magma, montrant que les points sont indépendants dans $E_{5,11}$. Par conséquent, le rang de $E_{t,k}$ est ≥ 5. □

3.3 Sous Famille infinie de Courbes Elliptiques possédant une Suite Arithmétique de longueur 7

On dit que les points $P(x_i, y_i)$, $i = 1, ..., k$ d'une courbe elliptique forment une suite arithmétique de longueur k si l'un des ensembles $\{x_1, ..., x_k\}$ ou $\{y_1, .., y_k\}$ forment une suite arithmétique. Cet aspect a été étudié de manière approfondie par plusieurs

spécialistes tels que G. Camplbell [6], M. Ulas [44], A. J. MacLeod [25] et d'autres où ils ont construit des familles de courbes elliptiques (pas nécessairement sous la forme de Weierstrass) contenant des points avec une suite arithmétique de longueur allant jusqu'à 10,12 et 14.
Dans cette section, nous utiliserons les points à coordonnées entières qui appartiennent à $E_{a,b}$ pour construire une suite arithmétique de longueur 7. Par rapport d'autres résultats, la progression dans cet exemple n'est pas assez longue mais il est intéressant d'obtenir la longueur 7 qui n'est pas évidente avec une méthode élémentaire. supposons que $a > b > 0$, on commence par réarranger les points à coordonnées entières par leur abscisse x.

$$\begin{aligned} x(P_2) &= \quad a+b, \\ x(P_3) &= \quad a-b, \\ x(P_0) &= \quad 0, \\ x(P_4) &= -a+b, \\ x(P_5) &= -a-b. \end{aligned}$$

Nous remarquons que la différence entre $x(P_2) = a + b$ et $x(P_3) = a - b$ est égale à $2b$. De même, cette différence apparaît également pour $x(P_4) = -a + b$ et $x(P_5) = -a - b$. Faisons la même différence entre chaque deux points. En fait, Nous devons donc juste résoudre l'équation

$$a - b = 2b.$$

La solution $a = 3b$ implique une suite arithmétique de longueur 5

$$\begin{aligned} x(P_2) &= \quad 4b, \\ x(P_3) &= \quad 2b, \\ x(P_0) &= \quad 0, \\ x(P_4) &= -2b, \\ x(P_5) &= -4b, \end{aligned}$$

dans la courbe elliptique d'équation $E_b : y^2 = x^3 + 9b^2x^2 - (10b^2)x + b^2$.
Il faut mentionner ici que la courbe elliptique obtenue E_b a encore plus de points entiers que sa précédente $E_{a,b}$ et ce jusqu'à 13, en comptant leur symétrique et le point à l'infini

O, la courbe E_b a au total les 27 points entiers (O et $\pm P_i : i = 0, ..., 12$) de coordonnés

$$\begin{aligned}
P_0 &= (0, b),\\
P_1 &= (1, 1),\\
P_2 &= (4b, 12b^2 + b),\\
P_3 &= (2b, 6b^2 - b),\\
P_4 &= (-2b, 6b^2 + b),\\
P_5 &= (-4b, 12b^2 - b),\\
P_6 &= (-8b^2 - 2b, -8b^3 + 6b^2 + b),\\
P_7 &= (-8b^2 + 2b, -8b^3 - 6b^2 + b),\\
P_8 &= (8b + 1, -24b^2 - 12b - 1),\\
P_9 &= (-8b + 1, 24b^2 - 12b + 1),\\
P_{10} &= (72b^2 - 6b, 648b^3 - 78b^2 + b),\\
P_{11} &= (72b^2 + 6b, -648b^3 - 78b^2 - b),\\
P_{12} &= (16b^2, -80b^3 + b).
\end{aligned}$$

Retour à notre progression arithmétique. Afin d'augmenter la longueur de la suite, nous imposons un point d'abscisse supplémentaire $6b$ dans E_b, ce qui signifie que $(156b + 324b^2 + 1)$ est un carré rationnel parfait. Ainsi, pour la solution paramétrique $b = \dfrac{(2k + 156)}{(k^2 - 324)}$, E_b se réduit à

$$E_k : y^2 = x^3 + 9\left(\frac{2k + 156}{k^2 - 324}\right)^2 x^2 - 10\left(\frac{2k + 156}{k^2 - 324}\right)^2 x + \left(\frac{2k + 156}{k^2 - 324}\right)^2,$$

et contient les points suivants dont les coordonnées x forment une suite arithmétique de longueur 6

$$\begin{aligned}
x(Q_1) &= 6\left(\tfrac{2k+156}{k^2-324}\right),\\
x(P_2) &= 4\left(\tfrac{2k+156}{k^2-324}\right),\\
x(P_3) &= 2\left(\tfrac{2k+156}{k^2-324}\right),\\
x(P_0) &= 0,\\
x(P_4) &= -2\left(\tfrac{2k+156}{k^2-324}\right),\\
x(P_5) &= -4\left(\tfrac{2k+156}{k^2-324}\right).
\end{aligned}$$

De même, nous pouvons imposer le point avec l'abscisse $8\left(\frac{2k+156}{k^2-324}\right)$ et pour cela il faut que $(k^4+864k^3+69048k^2+79488k-7712496)$ soit un carré rationnel parfait. La courbe elliptique $y^2+xy=x^3-4490x+96292$ associée à la dernière courbe hyperelliptique a le rang égale à 2 tel que calculé par Magma. On obtient donc une infinité de courbes elliptiques avec une suite arithmétique de longueur 7 paramétrées par une courbe elliptique quartique de rang positif.

Chapitre 4

Équations Diophantiennes et Courbes Elliptiques

4.1 Introduction et Résultats

Dans ce chapitre nous utilisons dans une partie la théorie des courbes elliptiques pour améliorer les résultat dans [50], puis via la théorie élémentaires des nombres, nous résolvons complètement le problème posé par M. Ulas et A. Togbé dans [45]. Il s'agit des solutions rationnelles des équations Diophantiennes $f(x)^2 \pm f(y)^2 = z^2$.
Soit $f(x) \in Q[x]$ un polynôme sans racines multiples et considérons les équations Diophantiennes

$$f(x)^2 + f(y)^2 = z^2 \tag{4.1}$$

et

$$f(x)^2 - f(y)^2 = z^2. \tag{4.2}$$

Le problème remonte à 2010 lorsque M. Ulas et A. Togbé [45] ont montré que si $f(x)$ est de degré 2, alors l'ensemble des solutions paramétriques rationnelles des équations

$$f(x)^2 \pm f(y)^2 = z^2 \tag{4.3}$$

est non vide et si $deg(f) = 3$ et f a la forme $f(x) = x(x^2 + ax + b)$ avec $a \neq 0$ alors (4.3) a une infinité de solutions paramétriques rationnelles non triviales, les auteurs ont également démontré le même résultat pour des polynômes cubiques plus généraux de la forme $f(x) = x^3 + ax^2 + b$ avec $b \neq 0$ pour l'équation (4.2) et ils se sont demandé s'il existe un polynôme de degré supérieur (> 3) tel que l'une ou les deux équations (4.1) et (4.2) soient satisfaites pour une infinité de solutions rationnelles non triviales (x, y, z).

Nous devrions également mentionner un article étroitement lié de Sz. Tengely et M. Ulas [42] dans lequel ils ont étudié l'existence de solutions intégrales des équations diophantiennes $z^2 = f(x)^2 \pm g(y)^2$ pour certains polynômes $f; g \in Z[x]$ de degré ≥ 3. Récemment, en octobre 2018, Y. Zhang et A. S. Zargar [50] ont répondu à la question d'Ulas et Togbé en utilisant une famille de polynômes quartiques. Nous avons amélioré le travail de [50] en prouvant pour certains polynômes de degré $2n+3$ ($n \in \mathbb{N}$) que les deux équations (4.1) et (4.2) possèdent une infinité de solutions rationnelles non triviales paramétrées par certaines courbes elliptiques sous un modèle quartique de rang positif, puis, par une méthode élémentaire, nous généralisons le résultat et résolvons le problème de manière différente en utilisant une famille de polynômes $f(x)$ de degré quelconque n pour les deux équations (4.1) et (4.2) en montrant qu'il existe une infinité de solutions rationnelles non triviales paramétrées par certaines coniques. En d'autres termes, nous avons prouvé les théorèmes suivants :

Théorème 38. *Soit*

$$f(x) = x\left(\prod_{t=0}^{n}(x-k^t)(x+k^t)\right).$$

Pour $k = \left(\frac{2h}{h^2-1}\right)$ *et* $h \neq 0, \pm 1$ *l'équation Diophantienne* $f(x)^2 + f(y)^2 = z^2$ *possède une infinité de solutions rationnelles non triviales.*

Théorème 39. *Soit*

$$f(x) = x\left(\prod_{t=0}^{n}(x-k^t)(x+k^t)\right).$$

Pour $k = \left(\frac{2h}{h^2+1}\right)$ *et* $h \neq 0, \pm 1$ *l'équation Diophantienne* $f(x)^2 - f(y)^2 = z^2$ *possède une infinité de solutions rationnelles non triviales.*

Théorème 40. *Soit*

$$f(x) = x\left(\prod_{t=0}^{n}(x+k^t)\right).$$

Pour $k = \left(\frac{2h}{h^2-1}\right)$ *et* $h \neq 0, \pm 1$ *l'équation Diophantienne* $f(x)^2 + f(y)^2 = z^2$ *possède une infinité de solutions rationnelles non triviales.*

Théorème 41. *Soit*

$$f(x) = x\left(\prod_{t=0}^{n}(x+k^t)\right).$$

Pour $k = \left(\frac{2h}{h^2+1}\right)$ *et* $h \neq 0, \pm 1$ *l'équation Diophantienne* $f(x)^2 - f(y)^2 = z^2$ *possède une infinité de solutions rationnelles non triviales.*

Nous rappelons qu'une solution (x, y, z) de (4.3) est dite non triviale si $f(x) \neq f(y)$, $f(x)f(y) \neq 0$ et $f(y) \neq 0$, sous ces conditions, nous prouvons ces théorèmes en utilisant

des transformations appropriées pour réduire le problème à la recherche de solutions sur certaines courbes elliptiques (quartiques) ou coniques. Avant de prouver les Théorèmes (38) et (39), le lemme suivant sera utile.

Lemme 42. *Soit $C : v^2 = au^4 + bu^2 + c^2$ une courbe hyper-elliptique définie sur $\mathbb{Q}$ tel que :*

$$\begin{cases} a \neq 0, c \neq 0 \\ a \text{ et } (b^2 - 4ac^2) \text{ ne sont pas des carrés rationnels} \end{cases}$$

alors

1. *La courbe hyper-elliptique C est bi-rationnellement équivalente à une courbe elliptique d'équation de Weierstrass*

$$E : y^2 = x^3 + bx^2 + ac^2x.$$

2. *La courbe elliptique associée à C possède un sous groupe de torsion isomorphe à $\frac{\mathbb{Z}}{2\mathbb{Z}}$.*

Démonstration. 1. En multipliant les deux côtés de C par a^2u^2, nous obtenons

$$(auv)^2 = (au^2)^3 + b(au^2)^2 + ac^2(au^2),$$

cela montre que C est bi-rationnellement équivalente à la courbe elliptique E donnée par l'équation de Weierstrass

$$E : y^2 = x^3 + bx^2 + ac^2x.$$

Pour en savoir plus de la façon de transformer l'équation d'une courbe elliptique du modèle cubique de Weierstrass au modèle quartique et vis-versa, reportez-vous à ([46] page 37 et à [29]).

2. On sait que ce modèle de courbe hyper-elliptique possède un sous-groupe de torsion parmi $\frac{\mathbb{Z}}{2\mathbb{Z}}$, $\frac{\mathbb{Z}}{2k\mathbb{Z}}$ et $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2k\mathbb{Z}}$ pour un entier pair k.
Le point $(x, y) = (0, 0)$ est dans E et puisque $y = 0$, ce point est d'ordre deux. Pour éliminer les groupes de la forme $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2k\mathbb{Z}}$, nous devons prouver que $(0, 0)$ est le seul point d'ordre deux. En effet, le second membre de E se factorise $x(x^2 + bx + ac^2)$ et le polynôme $(x^2 + bx + ac^2)$ est irréductible dans $\mathbb{Q}[x]$ puisque $b^2 - 4ac^2$ (discriminant de $x^2 + bx + ac^2$) d'après les conditions du lemme n'est pas censé être un carré rationnel. Pour terminer la preuve, nous devons également

s'assurer que E n'a pas de point d'ordre quatre. Si un point $P = (Z, W)$ est dans E alors la coordonnée x de $2P$ est

$$\frac{(Z^2 - (ac^2))^2}{4W^2}.$$

De cette manière, si P est d'ordre quatre, alors $2P$ est d'ordre 2 et donc $x(2P) = x(0, 0) = 0$, ce qui signifie $Z^2 = (ac^2)$ mais selon les conditions du Lemme.(42) le rationnel (a) n'est pas un carré. Par conséquent, E ne peut avoir un point d'ordre quatre et le sous-groupe de torsion de E ne peut être que $\frac{\mathbb{Z}}{2\mathbb{Z}}$.

□

4.2 Preuves des Théorèmes

Dans la section suivante, nous montrons que la méthode utilisée dans [50] pour prouver les théorèmes avec des polynômes de degré 4 reste valable pour certains polynômes de degrés $2n + 3$.

4.2.1 Preuve du Théorème (38)

Soit $k \neq 0, \pm 1$ et

$$f(x) = x \left(\prod_{t=0}^{n} (x - k^t)(x + k^t) \right). \tag{4.4}$$

En substituant

$$x \mapsto T \text{ et } y \mapsto kT, \tag{4.5}$$

l'équation (4.1) mène à

$$\begin{aligned}
z^2 = & \left(T \left(\prod_{t=0}^{n} (T - k^t)(T + k^t) \right) \right)^2 + \left(kT \left(\prod_{t=0}^{n} (kT + k^t)(kT + k^t) \right) \right)^2 \\
z^2 = & \left((T - k^n)(T + k^n) \left(T \left(\prod_{t=0}^{n-1} (T - k^t)(T + k^t) \right) \right) \right)^2 \\
& + \left(k^{2n+1}(kT - 1)(kT + 1) \left(T \left(\prod_{t=1}^{n} (T - k^{t-1})(T + k^{t-1}) \right) \right) \right)^2 \\
z^2 = & M^2 \left(((T - k^n)(T + k^n))^2 + (k^{2n+1}(kT - 1)(kT + 1))^2 \right) \\
z^2 = & M^2 \left((k^4 k^{4n+2} + 1)T^4 - 2k^{2n}(k^4 k^{2n} + 1)T^2 + (k^{4n} + k^{4n+2}) \right),
\end{aligned}$$

où

$$M = \left(T\left(\prod_{t=0}^{n-1}(T-k^t)(T+k^t)\right)\right) = \left(T\left(\prod_{t=1}^{n}(T-k^{t-1})(T+k^{t-1})\right)\right). \tag{4.6}$$

considérons maintenant la courbe

$$C_{1,k} = (k^4k^{4n+2}+1)T^4 - 2k^{2n}(k^4k^{2n}+1)T^2 + (k^{4n}+k^{4n+2}).$$

En mettant $k = \frac{2h}{h^2-1}$, le coefficient du monôme de degré zéro de $C_{1,k}$ devient un carré rationnel parfait, ce qui réduit $C_{1,k}$ à

$$\begin{aligned} C_{1,h} = \quad & \left((\frac{2h}{h^2-1})^{4n+6}+1)\right)T^4 - \left(2\left(\frac{2h}{h^2-1}\right)^{2n}\left(\left(\frac{2h}{h^2-1}\right)^{2n+4}+1\right)\right)T^2 \\ & + \left((\frac{2h}{h^2-1})^{4n} + (\frac{2h}{h^2-1})^{4n+2}\right). \end{aligned}$$

Par le Lemme (42) la courbe elliptique E associée à $C_{1,h}$ possède un sous groupe de torsion isomorphe à $\frac{\mathbb{Z}}{2\mathbb{Z}}$ où le point $\left(0, \frac{(h^2+1)^2(\frac{2h}{h^2-1})}{(h-1)^2(h+1)^2}\right)$ respectivement $\left(0, -\frac{(h^2+1)^2(\frac{2h}{h^2-1})}{(h-1)^2(h+1)^2}\right)$ dans $C_{1,h}$ correspond dans E au point $(x,y) = \infty$ (point à l'infini) respectivement à l'unique point de torsion non trivial dans E (d'ordre 2). Par conséquent, les points restants de $C_{1,h}$ comme

$$\left(\frac{h^2-1}{2h}, \frac{1}{4h^2}\left(-4h^2(2(\frac{2h}{h^2-1}))^{2n} - 2h^2 + h^4 + 1\right)\right)$$

par exemple, correspondent certainement à des points d'ordre infini dans E ce qui prouve la positivité du rang.
Enfin, l'équation (4.1) contient une infinité de solutions rationnelles non triviales.

4.2.2 Preuve du Théorème (39)

Pour $f(x)$ comme dans (4.4) et la substitution (4.5), l'équation (4.2) se réduit à

$$\begin{aligned} z^2 &= M^2\left(((T-k^n)(T+k^n))^2 - \left(k^{2n+1}(kT-1)(kT+1)\right)^2\right) \\ &= M^2\left((1-k^{4n+6})T^4 + 2k^{2n}(k^{2n+4}-1)T^2 + (k^{4n}-k^{4n+2})\right) \end{aligned}$$

où $M = \left(T\left(\prod_{t=0}^{n-1}(T-k^t)(T+k^t)\right)\right) = \left(T\left(\prod_{t=1}^{n}(T-k^{t-1})(T+k^{t-1})\right)\right).$

Considérons

$$C_{2,k}(T) = (1 - k^{4n+6})T^4 + 2k^{2n}(k^{2n+4} - 1)T^2 + (k^{4n} - k^{4n+2})$$

où $k = \frac{2h}{h^2+1}$. Maintenant, nous devons prouver que la courbe hyper-elliptique obtenue $C_{2,h}$ a un rang positif. En effet, en utilisant le même argument que dans l'équation (4.1), il suffit de trouver un point dans $C_{2,h}(T)$ autre que celui avec la coordonnée $x = 0$. Le point

$$\left(\frac{(h^2+1)}{2h}, \frac{1}{4h^2}\left(-4h^2\left(\frac{2h}{(h^2+1)}\right)^{2n} + (h^2+1)^2\right)\right)$$

correspond à ce que nous recherchons, donc la courbe elliptique correspondante de $C_{2,h}(T)$ a un rang positif et l'équation (4.2) a donc une infinité de solutions rationnelles non triviales.

4.2.3 Preuve du Théorème (40)

Dans cette partie, nous montrons que l'équation (4.1) contient une infinité de solutions rationnelles non triviales (x, y, z).
Considérons le polynôme sans racines multiples

$$f(x) = x\left(\prod_{t=0}^{n}(x + k^t)\right).$$

En posant $(x \mapsto T)$ et $(y \mapsto kT)$ l'équation (4.1) se réduit à

$$\begin{aligned} z^2 = &\left(T\left(\prod_{t=0}^{n}(T + k^t)\right)\right)^2 + \left(kT\left(\prod_{t=0}^{n}(kT + k^t)\right)\right)^2 \\ z^2 = &\left((T + k^n)\left(T\left(\prod_{t=0}^{n-1}(T + k^t)\right)\right)\right)^2 + \left(k^{n+1}(kT + 1)\left(T\left(\prod_{t=1}^{n}(T + k^{t-1})\right)\right)\right)^2, \end{aligned}$$

puisque nous avons l'égalité suivante

$$\left(T\left(\prod_{t=0}^{n-1}(T + k^t)\right)\right) = \left(T\left(\prod_{t=1}^{n}(T + k^{t-1})\right)\right) \tag{4.7}$$

l'équation (4.1) peut s'écrire sous la forme

$$z^2 = \left(T\left(\prod_{t=0}^{n-1}(T + k^t)\right)\right)^2 \left((T + k^2)^2 + k^{n+1}(kT + 1)^2\right).$$

Maintenant, il est clair que l'existence d'une solution de (4.1) dépend de la solvabilité de la conique

$$\begin{aligned} H_k(T) &= (T+k^2)^2 + k^{n+1}(kT+1)^2 \\ H_k(T) &= (k^{2n+4}+1)T^2 + (2k^{2n+3}+2k^n)T + (k^{2n}(k^2+1)). \end{aligned} \tag{4.8}$$

En mettant $k = \dfrac{2h}{h^2-1}$, le dernier coefficient de (4.8) devient un carré rationnel parfait qui, dans ce cas, $T = 0$ est une solution de $(H_h(T) = \square)$ cela implique qu'il existe une infinité de solutions rationnelles non triviales de $(H_h(T) = \square)$ et par conséquent, (4.1) possède une infinité de solutions rationnelles non triviales.

4.2.4 Preuve du Théorème (41)

En Utilisant le même polynôme

$$f(x) = x\left(\prod_{t=0}^{n}(x+k^t)\right)$$

et avec les mêmes transformations

$$x \mapsto T \text{ et } y \mapsto kT$$

l'équation (4.2) devient

$$\begin{aligned} z^2 = &\left(T\left(\prod_{t=0}^{n}(T+k^t)\right)\right)^2 - \left(kT\left(\prod_{t=0}^{n}(kT+k^t)\right)\right)^2 \\ z^2 = &\left((T+k^n)\left(T\left(\prod_{t=0}^{n-1}(T+k^t)\right)\right)\right)^2 - \left(k^{n+1}(kT+1)\left(T\left(\prod_{t=1}^{n}(T+k^{t-1})\right)\right)\right)^2 \end{aligned}$$

et (4.7) implique

$$z^2 = \left(T\left(\prod_{t=0}^{n-1}(T+k^t)\right)\right)^2 \left((T+k^2)^2 - k^{n+1}(kT+1)^2\right).$$

Considérons

$$\begin{aligned} D_k(T) &= (T+k^2)^2 - k^{n+1}(kT+1)^2 \\ &= (1-k^{2n+4})T^2 + (2k^n - 2k^{2n+3})T + (k^{2n}(1-k^2)), \end{aligned}$$

la substitution $k = \dfrac{2h}{h^2+1}$ rend le dernier coefficient de $D_h(T)$ un carré parfait, nous avons donc $T = 0$ une solution de la conique ($D_h(T) = \square$) et par conséquent, cette conique et l'équation (4.2) ont une infinité de solutions rationnelles non triviales.

Chapitre 5

Courbe Elliptique impliquant des sous familles de Rang au moins 5 sur $\mathbb{Q}(t)$ ou $\mathbb{Q}(t,k)$

Motivés par les travaux de Zargar et Zamani, nous introduisons une nouvelle famille de courbes elliptiques contenant plusieurs sous-familles à un paramètre (respectivement deux paramètres) de grand rang sur le corps de fonction $\mathbb{Q}(t)$ (respectivement $\mathbb{Q}(t,k)$). La nouvelle courbe elliptique que nous allons présenté peut être vu comme une généralisation de la courbe donnée par l'équation $E : (y-s)(y+s) = x(x-r)(x+r)$ dans [49]. Suivant l'approche de Moody [28] :

1. Nous construisons deux sous-familles infinies de courbes elliptiques de rang au moins 5 sur $\mathbb{Q}(t,k)$.
2. Nous déduisons deux autres sous-familles infinies de cette courbe elliptique induites par les bords d'un cuboïde rationnel et contenant cinq points $\mathbb{Q}(t)$-rationnels indépendants
3. Nous donnons une nouvelle sous-famille infinie induite par des triplets diophantiens rationnels de rang au moins 5 sur $\mathbb{Q}(t)$.
4. Par spécialisation, nous obtenons quelques exemples spécifiques de courbes elliptiques sur $\mathbb{Q}$ avec un rang élevé allant jusqu'à (8, 9, 10 et 11).

L'un des outils les plus puissants pour calculer une borne inférieure du rang d'une courbe elliptique sur le corps de fonctions est le théorème de spécialisation de Silverman [38], qui stipule que si un ensemble de N points $\mathbb{Q}(t)-$rationnels d'une courbe elliptique définie sur le corps de fonctions $\mathbb{Q}(t)$ sont indépendants pour une seule valeur de t alors ils resteraient ainsi pour tous sauf un nombre fini de valeurs t. (À notre connaissance, il

n'y a aucun moyen de déterminer ces valeurs exceptionnelles en général). Pour rechercher des courbes elliptiques de grand rang, on construit généralement des familles infinies ayant un rang générique suffisamment grand puis on essaie par spécialisation de trouver dans ces familles des courbes de rang particulièrement élevé en utilisant par exemple la somme de Mestre-Nagao [27, 32, 33]. Dans ce travail, nous utilisons une procédure très simple à partir d'une famille de rang générique connu, nous imposons un point d'abscisse donnée en faisant les changements de paramètres nécessaires pour que le point serait dans la courbe, ensuite nous vérifions son indépendance par rapport aux points génériques. Cette procédure peut être répétée pour augmenter le rang de 1 à chaque fois. Il y a une certaine difficulté dans la répétition de notre procédure, qui dépend du choix du point de départ et nous aurons donc des fonctions plus compliquées à traiter. Dans notre cas, 3 points ont été imposés et parmi les courbes résultantes, une d'entre elles semble être utile pour trouver des courbes de rang élevé sur $\mathbb{Q}$.

5.1 La courbe Elliptique $E_{a,b,c}$

Dans [49], les auteurs donnent quelques heuristiques sur la courbe elliptique

$$E_{(r,s)} : (y-r)(y+r) = x(x-s)(x-s), \tag{5.1}$$

qui contient plusieurs sous-familles de rang 4, 5 sur $\mathbb{Q}(t)$ et 6 (paramétrées par une courbe elliptique de rang positif) et construit une nouvelle sous-famille de cet courbe. Dans cette section, nous traitons une courbe elliptique similaire qui peut être vue comme une généralisation de (5.1), elle est donnée par l'équation

$$E_{(a,b,c)} : (y-h)(y+h) = (x-a^{\alpha})(x-b^{\beta})(x-c^{\gamma}), \tag{5.2}$$

où $a, b, c \in \mathbb{Q}(t)$ ou $\mathbb{Q}(t,k)$, $h = a^l b^m c^n$ et (l, m, n, α, β et γ sont des entiers positifs). Ce qui rend la famille $E_{(a,b,c)}$ intéressante, c'est qu'elle possède plusieurs différentes sous-familles de rang allant jusqu'à 5 sur $\mathbb{Q}(t)$ ou $\mathbb{Q}(t,k)$. Dans [28], les auteurs construisent deux sous-familles de $E_{(a,b,c)}$ de rang ≥ 5 sur $\mathbb{Q}(t)$ dont la première est donnée par l'équation

$$y^2 = x(x-a^2)(x-b^2) + a^2b^2,$$

ce qui correspond à

$$E_{(a,b,0)} : (y-ab)(y+ab) = x(x-a^2)(x-b^2). \tag{5.3}$$

La seconde utilise une nouvelle paramétrisation des longueurs des bords d'un cuboïde rationnel pour construire une sous-famille de

$$y^2 = (x - c^2)(x - a^2)(x - b^2) + a^2b^2b^2$$

de rang ≥ 5, en termes de notre nouvelle courbe elliptique elle correspond à

$$E_{(a,b,c)} : (y - abc)(y + abc) = (x - a^2)(x - b^2)(x - c^2). \tag{5.4}$$

Dans la section suivante, nous construisons deux nouvelles sous-familles de haut rang de $E_{(a,b,c)}$ sur $Q(t, k)$

5.2 Sous Familles de Rang ≥ 5 sur $\mathbb{Q}(t, k)$

5.2.1 Première sous famille de $E_{(a,b,c)}$

Nous traitons le cas où :

$$\begin{cases} h = a \\ c = 0 \end{cases} \tag{5.5}$$

Sous ces conditions, nous allons étudié la courbe elliptique donnée par

$$E^1_{(a,b)} : (y - a)(y + a) = x(x - a)(x - b). \tag{5.6}$$

Rang Générique

La courbe elliptique (5.6) peut s'écrire sous la forme

$$E^1_{(a,b)} : y^2 = x(x - a)(x - b) + a^2.$$

Ici, l'étude ne concerne pas le cas où la courbe est singulière.
Nous voyons que les points $P_0 = (0, a)$, $P_1 = (a, a)$ et $P_2 = (b, a)$ sont dans la courbe elliptique $E_{(a,b)}$ et comme ils sont colinéaire, seulement deux d'entre-eux peuvent être indépendants, comme on le verra en utilisant le théorème de spécialisation [38]. Quand on spécialise (a, b) à $(2, 3)$ nous obtenons un ensemble de trois points

$$P_0 = (0, 2), \quad P_1 = (2, 2) \text{ et } P_2 = (3, 2)$$

dans la courbe elliptique

$$E^1_{(2,3)} : y^2 = x(x-2)(x-3) + 4.$$

En utilisant MAGMA [2], on peut facilement vérifier que le régulateur de $P_1 = (2, 2)$ et $P_2 = (3, 2)$ est non nul $\simeq 0{,}44562252687009282459533230 1823$ montrant que ces deux points sont indépendants et donc $E_{(2,3)}$ est de rang ≥ 2.

Sous famille de rang 3

Afin d'augmenter le rang, nous allons extraire une sous-famille qui contient un point supplémentaire P_3 de sorte que P_1, P_2 et P_3 soient indépendants. Pour se faire, nous imposons un autre point à $E_{(a,b)}$ avec la coordonnée en x égale à $a + b$ ce qui implique que

$$a^2b + a^2 + ab^2$$

est un carré rationnel parfait, un calcul simple montre que

$$b = \frac{a(a+2r)}{(-a+r^2)}$$

fait partie des solutions paramétriques possibles.
D'où le point

$$P_3 = \left(ar\frac{(r-2)}{(-a+r^2)}, \frac{a(a+ar+r^2)}{(a-r^2)} \right)$$

est un point rationnel de la famille

$$F^1_{(a,r)} : y^2 = x^3 + \frac{ar(r+2)}{(a-r^2)}x^2 + \frac{a^2(a+2r)}{(-a+r^2)}x + a^2. \tag{5.7}$$

Par spécialisation à $(a, r) = (5, 4)$ les trois points $P_1 = (5, 5)$, $P_2 = (-45, 5)$ et $P_3 = (-40, 95)$ qu'ils sont dans la courbe elliptique résultante

$$y^2 = x^3 + 40x^2 - 225x + 25$$

sont indépendants car ils ont un régulateur non nul egal à $3,9189986763237144548844021 5771$ tel que calculé par Magma. Par conséquent, le rang est ≥ 3.

Sous famille de rang 4

Nous continuons la procédure en forçant un autre point d'abscisse $\dfrac{(a-r^2)}{(a-2r)}$ à être sur la courbe. Cela peut être effectuer lorsque

$$\frac{(a-r^2)}{(a-2r)}$$

est un carré rationnel parfait, disons t^2, une solution paramétrique est donnée par

$$a = r\frac{(-r+2t^2)}{(t-1)(t+1)}.$$

Nous arrangeons la courbe avec les nouveaux paramètres pour obtenir la sous-famille d'équation

$$G^1_{(t,r)} : y^2 = x^3 + \left(\frac{r(r-2t^2)}{(t^2)}\right)x^2 + \left(-\frac{r^2(r-2t^2)^2}{t^2(t-1)^2(t+1)^2}\right)x + \left(\frac{r(-r+2t^2)}{(t-1)(t+1)}\right)^2, \quad (5.8)$$

qui contient les points

$$\begin{aligned}
P_1 &= \left(\frac{r(-r+2t^2)}{(t-1)(t+1)}, \frac{r(-r+2t^2)}{(t-1)(t+1)}\right), \\
P_2 &= \left(\frac{r(r-2t^2}{t^2(t-1)(t+1)}, \frac{r(-r+2t^2)}{(t-1)(t+1)}\right), \\
P_3 &= \left(\frac{-r(r-2t^2)}{t^2}, \frac{r(r-2t^2)(r-t^2)}{t^2(t-1)(t+1)}\right), \\
P_4 &= \left(t^2, t(r-t^2)\right).
\end{aligned}$$

La spécialisation à $(t,r) = (5,3)$ donne la courbe elliptique

$$y^2 = x^3 - \frac{141}{25}x^2 - \frac{2209}{1600}x + \frac{2209}{64}.$$

Les points en questions $P_1 = (47/8, 47/8)$, $P_2 = (-47/200, 47/8)$,
$P_3 = (141/25, 517/100)$ et $P_4 = (25, -110)$ ont un régulateur égal à
147.475251328688414759767293294, Par conséquent, les points sont indépendants et la courbe à deux paramètres $G^1_{(t,r)}$ est de rang ≥ 4.

Sous famille de rang 5

Nous imposons un autre point d'abscisse $-\dfrac{r(r-2t^2)}{t^2(t-1)(t+1)}$ sur la courbe elliptique $G^1_{(t,r)}$. Par conséquent, nous voulons que

$$(-4rt^2+2r^2+t^6)$$

soit un carré rationnel parfait. En effet, sur $\mathbb{Q}(t)$ la conique

$$2r^2-(4t^2)r+(t^6)=k^2$$

a une solution $(r,k)=(0,t^3)$, donc une solution paramétrique peut être donnée par

$$r=\frac{2t^2(kt-2)}{(k^2-2)}.$$

Cela donne une nouvelle sous-famille de courbes elliptiques $H^1_{(t,k)}$ d'équation

$$y^2=x^3-\left(\frac{4kt^2(k-t)(kt-2)}{(k^2-2)^2}\right)x^2-\left(\frac{16t^6k^2(k-t)^2(kt-2)^2}{(k^2-2)^4(t-1)^2(t+1)^2}\right)+\left(\frac{4t^4k(kt-2)}{(k^2-2)^2(t-1)(t+1)}\right). \tag{5.9}$$

Cette dernière sous-famille contient les cinq points $\mathbb{Q}(t,k)$-rationnels suivants :

$$\begin{aligned}
P_1 &= \left(\frac{4t^4k(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)},\frac{4t^4k(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)}\right),\\
P_2 &= \left(\frac{-4kt^2(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)},\frac{4t^4k(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)}\right),\\
P_3 &= \left(\frac{4kt^2(k-t)(kt-2)}{(k^2-2)^2},\frac{4kt^2(k-t)(kt-2)(-2kt+k^2+2)}{(k^2-2)^3(t-1)(t+1)}\right),\\
P_4 &= \left(t^2,\frac{-t^3(-2kt+k^2+2)}{(k^2-2)}\right),\\
P_5 &= \left(\frac{4kt^2(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)},\frac{16k^2t^6(kt-2)^2(k-t)^2(-4k+2t+k^2t)^2}{(k^2-2)^6(t-1)^2(t+1)^2}\right).
\end{aligned}$$

La spécialisation à $(t,k)=(11,17)$ montre que ces points sont :

$$\begin{aligned} P_1 &= \left(\frac{9209189}{82369}, \frac{9209189}{82369}\right), \\ P_2 &= \left(\frac{-76109}{82369}, \frac{9209189}{82369}\right), \\ p_3 &= \left(\frac{9133080}{82369}, \frac{764362687}{23639903}\right), \\ P_4 &= \left(121, \frac{110473}{287}\right), \\ P_5 &= \left(\frac{76109}{82369}, \frac{2622944467}{23639903}\right), \end{aligned}$$

sur la courbe spécialisée

$$H^1_{(11,17)} : y^2 = x^3 - \frac{9133080}{82369}x^2 - \frac{700902165601}{6784652161}x + \frac{848091620377 21}{6784652161}. \tag{5.10}$$

Le calcul par Magma du régulateur de l'ensemble $S=\{P_1,P_2,P_3,P_4,P_5\}$ révèle $R(S)\simeq 6915.28812722...$ ce qui implique l'indépendance de ces points et montre que la sous-famille $H^1_{(t,k)}(\mathbb{Q}(t,k))$ est de rang au moins 5.

5.2.2 Deuxième sous famille de $E_{(a,b,c)}$

L'étude de cette courbe est similaire à la première famille (5.6), donc certains détails seront omis.
Considérons la courbe elliptique donnée par

$$E^2_{(a,b)} : (y-ab)(y+ab) = x(x-ab)(x-b),$$

qui peut s'écrire sous la forme

$$E^2_{(a,b)} : y^2 = x(x-ab)(x-b) + (ab)^2. \tag{5.11}$$

En plus des trois points clairement visibles

$$(0,ab), (b,ab) \quad \text{et} \quad (ab,ab)$$

on commence par imposer :

Le premier point d'abscisse $ab + b$

Cela peut être réalisé lorsque

$$b = \frac{-(a-r)(a+r)}{a(a+1)}.$$

On obtient la courbe

$$F^2_{(a,r)} : y^2 = x\left(x - \frac{-(a-r)(a+r)}{(a+1)}\right)\left(x - \frac{-(a-r)(a+r)}{a(a+1)}\right) + \left(\frac{-(a-r)(a+r)}{(a+1)}\right)^2. \quad (5.12)$$

Le deuxième point d'abscisse $-a$

Pour cela, nous avons besoin de

$$a = -k^2$$

et l'équation sera de la forme

$$G^2_{(k,r)} : y^2 = x^3 + \left(\frac{-(k^4 - r^2)}{(k^2)}\right)x^2 + \left(\frac{-(r+k^2)^2(-r+k^2)^2}{k^2(k-1)^2(k+1)^2}\right)x + \left(\frac{(r+k^2)^2(-r+k^2)^2}{(k-1)^2(k+1)^2}\right). \quad (5.13)$$

Le troisième point d'abscisse $\dfrac{(r+k^2)(-r+k^2)}{(k-1)^2(k+1)^2}$

Pour forcer ce point à être dans la courbe, il faut montrer que la conique

$$t^2 = (2k^4 - 5k^2 + 2)r^2 + k^2(k + k^2 - 1)^2(-k + k^2 - 1)^2$$

possède une solution. En effet, sur $\mathbb{Q}(k)$ cet dernière possède la solution

$$(t, r) = (k(k + k^2 - 1)(-k + k^2 - 1), 0)$$

Par conséquent, une solution paramétrée peut être donnée par

$$r = \frac{2tk(-k + k^2 - 1)(k + k^2 - 1)}{(t^2 + 5k^2 - 2k^4 - 2)}.$$

Enfin, nous obtenons une courbe elliptique sur $\mathbb{Q}(t, k)$ d'équation

$$H^2_{(t,k)} : y^2 = x(x - ab)(x - b) + (ab)^2 \quad (5.14)$$

où

$$\begin{aligned} ab &= \frac{k^2(kt-5k^2+2k^4+2)(-kt-5k^2+2k^4+2)(k-t)(k+t)}{(-5k^2+2k^4-t^2+2)^2(k-1)(k+1)}, \\ b &= \frac{-(-kt-5k^2+2k^4+2)(kt-5k^2+2k^4+2)(k-t)(k+t)}{(-5k^2+2k^4-t^2+2)^2(k-1)(k+1)}, \\ a &= -k^2. \end{aligned}$$

qui contient cinq points $\mathbb{Q}(t,k)$-rationnels donnés par leur abscisses

$$\begin{aligned} x(P_1) &= 0, \\ x(P_2) &= \frac{(t+k)(-tk-5k^2+2k^4+2)(tk-5k^2+2k^4+2)(t-k)}{(t^2+5k^2-2k^4-2)^2(k-1)(k+1)}, \\ x(p_3) &= \frac{(t+k)(tk+5k^2-2k^4-2)(tk-5k^2+2k^4+2)(t-k)}{(t^2+5k^2-2k^4-2)^2}, \\ x(P_4) &= k^2, \\ x(P_5) &= \frac{k^2(t+k)(tk+5k^2-2k^4-2)(tk-5k^2+2k^4+2)(t-k)}{(t^2+5k^2-2k^4-2)^2}. \end{aligned}$$

Par spécialisation à $(t,k)=(2,3)$ on obtient la courbe elliptique

$$H^2_{(2,3)} : y^2 = x^3 - \frac{2825}{529}x^2 - \frac{71825625}{17909824}x + \frac{646430625}{17909824}.$$

Les points mentionnés ci-dessus sont

$$\begin{aligned} P_1 &= (0, 25425/4232), \\ P_2 &= (-2825/4232, 25425/4232), \\ P_3 &= (2825/529, 93225/24334), \\ P_4 &= (9, 396/23), \\ P_5 &= (25425/33856, 34400025/6229504). \end{aligned}$$

Leur régulateur calculé par Magma égal à 493.27438456129354050231958979 3 ce qui prouve leur indépendance.

5.3 Sous-familles de $E_{(a,b,c)}$ de rang au moins 5 provenant d'un cuboïde rationnel

Soit S un système formé de 3 équations Diophantiennes à 6 inconnues défini par

$$S = \begin{cases} x^2 + y^2 = Z^2, \\ x^2 + z^2 = Y^2, \\ y^2 + y^2 = X^2. \end{cases} \tag{5.15}$$

La recherche d'une solution rationnelle du système (5.15) est équivalent à la recherche d'un parallélépipède rectangle (cuboïde) dont les arêtes et les diagonales des faces sont toutes rationnelles. Un tel système possède de nombreuses solutions paramétriques qui peuvent être trouvées dans [28, 37, 9]. Si $[a, b, c]$ sont les arêtes d'un cuboïde rationnel, alors $[ka, kb, kc]$ $(k \in \mathbb{Q}^*)$ et $[ab, bc, ac]$ constituent également un cuboïde rationnel. Dans [28], il a été montré que si a, b et c sont les longueurs des bords d'un cuboïde rationnel, alors la courbe (5.4) a 5 points rationnels indépendants. En réalité, à partir de leur construction, on peut créer d'autres sous-familles de rang au moins 5 d'une manière très simple.

5.3.1 La 1$^{\text{ier}}$ sous famille Cub1

Soit

$$E^{Cub1}_{(a,b,c)} : (y - a^2b^2c^2)(y + a^2b^2c^2) = (x - a^2b^2)(x - a^2c^2)(x - b^2c^2)$$

qui peut s'écrire

$$E^{Cub1}_{(a,b,c)} : y^2 = (x - a^2b^2)(x - a^2c^2)(x - b^2c^2) + a^4b^4c^4. \tag{5.16}$$

Cette courbe a un sous-groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z}$ généré par $(0, 0)$.
Les trois points

$$P_0 = (b^2c^2, a^2b^2c^2),\ P_1 = (a^2b^2, a^2b^2c^2) \text{ et } P_2 = (a^2c^2, a^2b^2c^2)$$

se situent clairement sur la courbe, ils ne sont pas de torsion et comme ils sont colinéaires, au plus deux d'entre eux peuvent être indépendants. En considérant toute paramétrisation d'un cuboïde rationnel de longueurs a, b et c, trois autres points seront sur (5.16), à savoir

$$P_3 = ((ab)^2 + (ac)^2, a^3bcA),$$

$$P_4 = ((ab)^2 + (bc)^2, ab^3cC),$$

$$P_5 = ((ac)^2 + (bc)^2, abc^3B),$$

où

$$A^2 = b^2 + c^2, B^2 = a^2 + c^2 \text{ et } C^2 = a^2 + b^2$$

.

L'utilisation de l'une des paramétrisations de ([28], Section 3.1-(4))

$$\begin{aligned} a &= -2t^2(t^4-3)(3t^4-1), \\ b &= -8t^2(t^8-1), \\ c &= (t^4-1)(t^8-14t^4+1), \\ A &= (t^4-1)(t^8+18t^4+1), \\ B &= (t^4+1)^3, \\ C &= 2t^2(5t^8-6t^4+5), \end{aligned} \tag{5.17}$$

et par spécialisation à $t = 2$, (5.16) devient

$$E_2^{Cub1} : y^2 = x^3 - 1613068785000000x^2 + 353648093980462850805350400000x.$$

Les cinq points de la courbe résultante sont

$$\begin{aligned} P_1 &= (1590899377766400, 389810120037212160000), \\ P_2 &= (5854270593600, 38981012003721216000), \\ P_3 &= (1596753648360000, 3856352374384773120000), \\ P_4 &= (1607214514406400, 6458826768958586880000), \\ P_5 &= (22169407233600, 46015992586586880000), \end{aligned}$$

et ont un régulateur non nul $R = 952846.119732081738743944356546$ tel que calculé par Magma qui confirme que le rang est d'au moins 5.

5.3.2 La $2^{\text{ième}}$ sous famille Cub2

Une autre nouvelle sous-famille peut être donnée en considérant la courbe elliptique définie par

$$E^{Cub2}_{(a,b)} : y^2 = (x - a^2)(x - b^2)(x - a^2b^2) + a^4b^4. \tag{5.18}$$

En plus des trois points évidents

$$P_0 = (a^2b^2, a^2b^2), P_1 = (a^2, a^2b^2) \text{ et } P_2 = (b^2, a^2b^2),$$

trois autres points peuvent être imposés dans la courbe comme suit :
Soit $f(x)$ le deuxième membre de (5.18), alors

$$\begin{aligned} f(a^2 + b^2) &= a^2b^2(a^2 + b^2), \\ f(a^2 + a^2b^2) &= a^6b^2(b^2 + 1), \\ f(b^2 + a^2b^2) &= a^2b^6(a^2 + 1). \end{aligned} \tag{5.19}$$

A partir de (5.19) nous voyons que si 1, a et b sont des longueurs d'arêtes d'un cuboïde rationnel, les points d'abscisse $(a^2 + b^2)$, $(a^2 + a^2b^2)$ et $(b^2 + a^2b^2)$ sont dans la courbe. La multiplication par $1/c$ dans (5.17) donne une paramétrisation pour le cuboïde de longueurs 1, a and b

$$\begin{aligned} a &= \frac{(t^4 - 1)(t^8 - 14t^4 + 1)}{-2t^2(t^4 - 3)(3t^4 - 1)}, \\ b &= \frac{-8t^2(t^8 - 1)}{-2t^2(t^4 - 3)(3t^4 - 1)}, \\ c &= 1. \end{aligned} \tag{5.20}$$

Maintenant, montrons que les cinq points d'abscisse

$$a^2, b^2, (a^2 + b^2), (a^2 + a^2b^2) \text{ et } (b^2 + a^2b^2)$$

sont indépendants par spécialisation à $t = 2$ dans (5.20).
la courbe résultante est

$$E^{Cub2}_2 : y^2 = x^3 - \frac{25204199765625}{8919588418624} + \frac{1445469627586730625}{13319478672116521216}x$$

et les points sont

$$\begin{aligned}
P_{a^2} &= (245025/23892544, 15932750625/557474276164),\\
P_{b^2} &= (1040400/373321, 15932750625/557474276164),\\
P_{a^2+b^2} &= (66830625/23892544, 1031889375/3649586096),\\
P_{a^2+a^2b^2} &= (346396988025/8919588418624, 36773725663125/10899737047558528),\\
P_{b^2+a^2b^2} &= (1569545424225/557474276164, 40324826210625/85154195684051),
\end{aligned}$$

et ont un régulateur non nul égal à 952846.119732081738743944356548, donc les points sont indépendants et (5.18) est de rang au moins 5 sur $\mathbb{Q}(t)$.

5.4 Sous Familles de Rang ≥ 5 issues de Triplets Rationnels Diophantiens

Dans cette section, nous introduisons une nouvelle sous-famille de (5.2) issue des triplets diophantiens rationnels. Un ensemble de m entiers rationnels non nuls $\{a_1, a_2, ..., a_m\}$ est appelé un *m-Uplet Diophantien Rationnel* si $a_i a_j + 1$ est un carré rationnel parfait pour tous $1 \leq i < j \leq m$.
les m-Uplets Diophantiens rationnels ont été minutieusement étudiés par A. Dujella ([13, 12, 20, 16, 18]). Ici, nous utilisons des triplets avec cette propriété pour imposer 3 points sur la courbe elliptique

$$E^{Dio}_{(a,b)} : y^2 = (x-1)(x-a^2)(x-a^2b^2) + a^4b^2. \tag{5.21}$$

Les points

$$Q_0 = (a^2b^2, a^2b), Q_1 = (1, a^2b) \text{ et } Q_2 = (a^2, a^2b)$$

se situent clairement dans la courbe (5.21).
Notant que si les images par $g(x)$ (second membre de (5.21))

$$\begin{aligned}
g(a^2 + a^2b^2) &= a^6b^2(b^2+1),\\
g(a^2+1) &= a^2(a^2+1),\\
g(a^2b^2+1) &= a^2b^2(a^2b^2+1)
\end{aligned} \tag{5.22}$$

sont des carrés parfaits, les points d'abscisses

$$a^2+1,\ a^2b^2+1 \text{ et } a^2b^2+a^2$$

seront également dans la courbe. Pour que cela puisse arriver, nous devons résoudre le système d'équations Diophantiennes à 3 équations et à 5 inconnus

$$S' = \begin{cases} a^2+1=A^2, \\ b^2+1=B^2, \\ a^2b^2+1=C^2. \end{cases} \tag{5.23}$$

Ce problème est équivaut à trouver un triplet Diophantien rationnel de la forme $\{1, a^2, b^2\}$. Il possède plusieurs solutions rationnelles paramétriques, nous donnons deux d'entre-elles qui nous ont été communiquées par A. Dujella.
Pour $t \notin \left\{0, \pm 1, -\frac{1}{3}, \frac{1}{2}, -2, 3\right\}$

$$\begin{aligned} a &= \frac{4(t^2+1)(t^2-t-1)}{(t-1)(t-3)(3t+1)(t+1)}, \\ b &= \frac{(t^2+1)(t^2+4t-1)}{2t(t+2)(2t-1)}. \end{aligned} \tag{5.24}$$

Pour la second solution rationnelle paramétrique ($t \neq \pm 2$)

$$\begin{aligned} a &= \frac{(3t^2-4)(t^2-12)}{4(t-2)(t+2)(t^2+4)}, \\ b &= \frac{16t(t^2+4)}{(t^2-8t+4)(t^2+8t+4)}. \end{aligned} \tag{5.25}$$

En remplaçant a et b de (5.24) ou (5.25) dans la courbe (5.21), nous obtenons une sous-famille infinie de courbes elliptiques F_t^{Dio} qui contiennent les points mentionnés ci-dessus. Montrons maintenant que la sous-famille résultante a un rang supérieur ou égal à 5 sur $\mathbb{Q}(t)$ en prouvant l'indépendance des cinq points $\mathbb{Q}(t)$-rationnels d'abscisse

$$\begin{aligned} x(Q_1) &= 1, \\ x(Q_2) &= a^2, \\ x(Q_3) &= a^2+1, \\ x(Q_4) &= a^2b^2+1, \\ x(Q_5) &= a^2b^2+a^2. \end{aligned}$$

En se spécialisant à $t = 5$ dans (5.24), cela donne

$$a = 247/96,\ b = 572/315.$$

Pour ces valeurs, la courbe elliptique résultante est

$$F_5^{Dio}(\mathbb{Q}) : y^2 = x^3 - \frac{26929244281}{914457600}x^2 + \frac{3643908031465}{21069103104}x,$$

et les points sont

$$\begin{aligned}
Q_1 &= \left(1, \frac{8724287}{725760}\right), \\
Q_2 &= \left(\frac{61009}{9216}, \frac{8724287}{725760}\right), \\
Q_3 &= \left(\frac{70225}{9216}, \frac{65455}{9216}\right), \\
Q_4 &= \left(\frac{1304726641}{57153600}, \frac{1275829841}{57153600}\right), \\
Q_5 &= \left(\frac{26014786681}{914457600}, \frac{1407148974517}{21946982400}\right)
\end{aligned}$$

et ont un régulateur non nul égal à 798694.26174964901769224830787 0. Par conséquent, les points sont indépendants et le rang de F_t^{Dio} est d'au moins 5 sur $\mathbb{Q}(t)$.

5.5 Exemples de Courbes Elliptiques de grand Rang (Résultats Numériques)

Dans cette section, nous essayons par spécialisation de trouver des courbes elliptiques de grand rang en calculant $S(E, 10^5)$ en utilisant Pari-Gp [34] ce qui nous permet de repérer les meilleurs candidats. Pour aller plus loin dans le calcul, nous avons choisi la courbe (5.9) car ces coefficients augmentent d'une manière très faible par rapport aux autres courbes obtenues dans ce travail. Donc, pour la courbe (5.9) mettons $t = \frac{1}{k}$; ce qui donne une courbe définie sur $\mathbb{Q}(k)$, ce choix peut être justifie juste en regardant la taille des coefficients de la courbe obtenue

$$H^1_{(\frac{1}{k},k)} : y^2 = x^3 + \left(\frac{4(k-1)(k+1)}{k^2(k^2-2)^2}\right)x^2 + \left(\frac{-16}{k^2(k^2-2)^4}\right)x + \left(\frac{4}{k^2(k^2-2)^2}\right) \quad (5.26)$$

écrite sous son modèle intégral

$$I^1_{(k)} : y^2 = x^3 + (4k^2 - 4)x^2 - 16k^2x + 16k^2(k^2 - 2)^2, \tag{5.27}$$

que nous allons l'utilisé pour les calculs.
En utilisant Magma et Pari-Gp nous avons calculé $S(10^5, E)$ pour $1 \leq k \leq 100000$ et trouvé plusieurs courbes elliptiques de rang 7, 8 et 9, deux courbes de rang 10 et une seule de rang 11, les résultats sont listés dans le tableau suivant

TABLE 5.1 – High Rank Curves

$rank$	k
7	23, 38, 941, ...
8	82, 138, 502, ...
9	123, 309, 652, 707, 749, 901, 996, 1044, ...
10	5394, 24862
11	30422

Détails sur la courbe de rang 11 :
k :=30422 ;
Modèle minimal :
$E_{30422} : y^2 = x^3 - 285515568137723047x + 256903996022907086595281290.$
Groupe de torsion trivial.
Abscisses de 11 points indépendants :
$P_1 = \left(\frac{-60215388418841240}{14055001}\right)$,
$P_2 = \left(\frac{-24171054980237264268}{31633112449}\right)$,
$P_3 = \left(\frac{104817386986874324312}{111774542929}\right)$,
$P_4 = \left(\frac{-655026868908}{169}\right)$,
$P_5 = \left(\frac{-26621245519911112932312}{630561458241}\right)$,
$P_6 = \left(\frac{-55268374695346492531882184 0}{132719478771081409}\right)$,
$P_7 = \left(\frac{-135712128335}{36}\right)$,
$P_8 = \left(\frac{-2450470703286048}{10259209}\right)$,
$P_9 = \left(\frac{-4551146090623594003}{6055796761}\right)$,
$P_{10} = \left(\frac{1429511357792752}{292681}\right)$,
$P_{11} = 2^4 \times 7^2 \times 23 \times 41 \times 53 \times 1483 \times 42015019 \times$
$\frac{1121472433799 \times 23389711734370649 \times 2147894829893544830 9 \times 1155972852326767801424443563483954505087}{17^2 \times 3970506863^2 \times 907301670536311529740830643904251859 3^2}$.

Annexe

5.5.1 Calculs avec Pari-GP

Définir la somme $S(N, E)$:

S(E,N)=my(s=0.0) ;forprime(p=2,N,my(a=ellap(E,p)) ;s+=(2-a)*log(p)/(p+1-a)) ;return(s) ;

Lancer le calcul :

for(t=2,250,E=ellinit([a1(t),a2(t),a3(t),a4(t),a6(t)]) ;print(t," : ",S(E,10^6)))

5.5.2 Codes Magma fréquemment utilisés

Définir une courbe elliptique

E :=EllipticCurve($[a_1, a_2, a_3, a_4, a_6]$) ;

Déterminant

Determinant(E) ;

Régulateur

Regulator(E) ;

Sous Groupe de Torsion

TorsionSubgroup(E) ;

Points entiers

IntegralPoints(E) ;

Base de Points entiers

E :=EllipticCurve($[a_1, a_2, a_3, a_4, a_6]$) ;

I :=IntegralPoints(E) ;

ReducedBasis(I) ;

Ordre du groupe de Selmer

E :=EllipticCurve($[a_1, a_2, a_3, a_4, a_6]$) ;

SetClassGroupBounds("GRH") ;

two := MultiplicationByMMap(E,2) ;

mu, tor := DescentMaps(two) ;

S, AtoS := SelmerGroup(two) ;

[$\sharp S$,RankBound(E : Isogeny := two)] ;

end for ;

Corps de fonctions $\mathbb{Q}(t)$

Q<t> :=FunctionField(Rationals()) ;

Anneau de polynômes $P[X]$

P<x> :=PolynomialRing(Rationals()) ;

Rang d'une courbe elliptique E

Rank(E) ;

Informations sur le groupe de Mordell-Weil

DescentInformation(E) ;

Pour plus de commandes reportez vous à Magma hand book [2].

Conclusion et perspectives

Le fait que nombreux problèmes concernant le rang des courbes elliptiques demeurent sans réponses, attire de plus en plus les théoriciens des nombres à se pencher d'avantage sur l'étude de cet invariant.
Concernant l'existence d'une courbe elliptique de rang arbitraire, des spécialistes tels Silverman [39] et d'autres ont donnés des arguments qui donnent espoir à une réponse positive. D'un autre coté, d'autre spécialistes comme Park, Poonen, Voight et Woods dans [35] ont introduit un modèle probabiliste heuristique pour les rangs des courbes elliptiques qui suggère que les rangs sont bornés, de sorte qu'il y ait un nombre fini de courbes elliptiques sur $\mathbb{Q}$ de rang supérieur à 21.
Les courbes elliptiques de rang élevé possèdent généralement de très grands coefficients dépassant même les limites des calculateurs disponibles, il serait Donc nécessaire d'élaborer des méthodes alternatives pour éviter les lourds calculs.
Une de mes premières perspectives est de construire des courbes elliptiques qui possèdent plusieurs points dont les coordonnées forment une longue suite arithmétique, en effet, cette propriété implique que le rang du groupe de Mordell-Weil est grand.
Un deuxième point de vue que je soutient fortement découle de l'existence d'une infinité d'entiers positif M qui peuvent être écrits de n manières différentes $n \in \{2, 3\}$ comme somme de trois entiers positifs distincts ayant le même produit N. Trouver des entiers possédants plusieurs écritures implique un rang élevé de la courbe elliptique $E_{S,N} = y^2 - Mxy + Ny = x^3$, il serait interessant d'améliorer ce résultat.

Bibliographie

[1] J. Aguirre, A. Dujella, M.J. Bokun and J.C. Peral, High rank elliptic curves with prescribed torsion group over quadratic fields, Period. Math. Hungar, 68 (2), 222-230, 2014.

[2] W. Bosma, J.J. Cannon, C. Fieker and A. Steel (eds.), Handbook of Magma functions, Edition 2.20-9, 2014.

[3] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. vol. 109 (1), 445-472, 1992.

[4] J. P. Buhler, B. H. Gross, and D. B. Zagier, On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. Mathematics of Computation, 44(170), 473-481 (1985).

[5] G. Campbell, Finding elliptic curves and families of elliptic curves over $\mathbb{Q}$ of large rank, PhD Thesis, Rutgers University, 1999.

[6] G. Campbell, A note on arithmetic progressions on elliptic curves. J. Integer Seq. **6** no (3.1) (2003), 3.

[7] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London. Math. Soc. vol. 1 (1), 193-291, 1966.

[8] J. Cremona. (2016). ecdata : 2016-10-17. Zenodo. 10.5281/zenodo.161341.

[9] L.E. Dickson, History of the theory of numbers, Vol. II, Diophantine analysis, Dover Publications, New York, 2005.

[10] A. Dujella, An example of elliptic curve over $\mathbb{Q}$ with rank equal to 15, Proceedings of the Japan Academy, Series A, Mathematical Sciences, 78 (7), 109-111, 2002.

[11] A. Dujella, https ://web.math.pmf.unizg.hr/ duje/index.html.

[12] A. Dujella, On the number of Diophantine m-tuples, Ramanujan J, 15, 37-46, 2008.

[13] A. Dujella, On the size of Diophantine m-tuples, Math. Proc. Cambridge Philos. Soc, 132, 23-33,2002.

[14] A. Dujella and J.C. Peral, High rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples, LMS J. Comput. Math, 17, 282-288, 2014.

[15] A. Dujella and J.C. Peral. Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Trends in number theory, Contemp. Math, vol. 649, p. 47-62, 2015.

[16] A. Dujella and V. Petricevic, Strong Diophantine triples, Experiment. Math, 17, 83-89, 2008.

[17] S. Férmigier, Un exemple de courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 19. Comptes rendus de l'Académie des sciences. Série 1, Mathématique, 315(6), 719-722.

[18] A. Filipin and A. Togbé, On the family of Diophantine triples $\{k+2, 4k, 9k+6\}$, Acta Math. Acad. Paedagog. Nyhàzi. (N.S.) Vol. 25 (2), 145-153, 2009.

[19] W. Fulton, Algebraic curves : an introduction to algebraic geometry. Addison-Wesley, 1989.

[20] Bo He and A. Togbé, On the family of Diophantine triples $\{k+1, 4k, 9k+3\}$, Period. Math. Hungar, 58, 59-70, 2009.

[21] T. Honda, *Isogenies, rational points and section points of group varieties*, Japanese journal of mathematics :transactions and abstracts. Vol. 30, 84-101, 1960.

[22] Husemöller, D. (1987). Elliptic curves, volume 111 of. Graduate Texts in Mathematics, 99.

[23] C. G. J. Jacobi, De usu theoriae integralium ellipticorum et integralium Abelianorum in analysi Diophantea. Journal für die reine und angewandte Mathematik, 1835(13), 353-355.

[24] S. Kihara, (2000). On the rank of elliptic curves with a reational point of order 3. Proceedings of the Japan Academy, Series A, Mathematical Sciences, 76(8), 126-127.

[25] A. J. MacLeod, 14-term arithmetic progressions on quartic elliptic curves. J. Integer Seq. **9** no 1 (2006), article 06.1.2, 4.

[26] J.F. Mestre, Construction de courbes elliptiques sur $\mathbb{Q}$ de rang > 12, C. R. Acad. Sci. Paris Ser, I 295, 643644, 1982.

[27] J.F. Mestre, Courbes elliptiques de rang ≥ 11 sur $\mathbb{Q}(T)$, C. R. Acad. Sc. Paris, I 313, 139142, 1991.

[28] D. Moody, M. Sadek and A.S. Zargar, Families of elliptic curves of rank ≥ 5 over $\mathbb{Q}(t)$, Rocky Mountain Journal of Mathematics, 49 (7), 2253-2266, 2019.

[29] L.J. Mordell, Diophantine Equations, Pure and Applied Mathematics, vol. 30 (Academic, London, 1969).

[30] K. Nagao, An example of elliptic curve over $\mathbb{Q}$ with rank > 20, Proc. Japan Acad. Ser. A Math. Sci, 69, 291293, 1993.

[31] K. Nagao, An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 21, Proc. Japan Acad. Ser. A Math. Sci, 70, 104105, 1994.

[32] K. Nagao, Construction of high-rank elliptic curves. Kobe journal of mathematics, 11(2), 211-219, 1994.

[33] K. Nagao, $\mathbb{Q}(T)$-rank of elliptic curves and certain limit coming from the local points, manuscripta mathematica, 92(1), 13-32, 1997.

[34] The PARI Group, PARI/GP version `2.9.1`, Univ. Bordeaux, 2016, `http://pari.math.u-bordeaux.fr/`.

[35] J. Park, B. Poonen, J. Voight and M. M. Woods, A heuristic for boundedness of ranks of elliptic curves. arXiv preprint arXiv :1602.01431, 2016.

[36] D. E. Penney and C. Pomerance, (1974). A search for elliptic curves with large rank. Mathematics of Computation, 28(127), 851-853.

[37] N. Saunderson, The elements of algebra, Book 6, Cambridge University Press, Cambridge (1740).

[38] J.H. Silverman, Advanced topics in the arithmetic of elliptic curves, Vol 151, Springer Science and Business Media, 2013.

[39] Silverman, J. H. and Tate, J. T. (1992). Rational points on elliptic curves (Vol. 9). New York : Springer-Verlag.

[40] Silverman, J. H. (2009). The arithmetic of elliptic curves (Vol. 106). Springer Science and Business Media.

[41] J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. vol. 23 (3-4), 179-206, 1974.

[42] S.Tengely, M. Ulas, (2017). On certain Diophantine equations of the form z2= f (x) 2śg (y) 2. Journal of Number Theory, 174, 239-257.

[43] J. Top, Descent by 3-isogeny and 3-rank of quadratic fields. Advances in Number Theory. (1991), 303–317.

[44] M. Ulas, A note on arithmetic progressions on quartic elliptic curves. J. Integer Seq. **8** (3) (2005), art. 05.3.1, 5. Zbl 1022.11026.

[45] M. Ulas, A. Togbé, On the Diophantine equation $z^2 = f(x)^2 \pm f(y)^2$. Publ. Math. Debrecen 76(1-2), 183201 (2010).

[46] Washington, L. C. (2008). Elliptic curves : number theory and cryptography. CRC press.

[47] A. E. A. Youmbai and D. Behloul, Rational solutions of the diophantine equations $f(x)^2 \pm f(y)^2 = z^2$, Periodica Mathematica Hungarica 79 , no. 2, 255-260, 2019.

[48] A. E. A. Youmbai, A. M. Uludağ and D. Behloul, Elliptic curve involving subfamilies of rank at least 5 over $\mathbb{Q}(t)$ or $\mathbb{Q}(t, k)$, Hacettepe Journal of Mathematics and Statistics, vol. 50, no. 3, pp721-731 (2021).

[49] A.S. Zargar and N. Zamani, A Family of Elliptic Curves of Rank ≥ 5 over $\mathbb{Q}(m)$, Notes on Number Theory and Discrete Mathematics, 25 (4), 24-29, 2019, doi : 10.7546/nntdm.2019.25.4.24-29.

[50] Y. Zhang, A. S. Zargar. "On the Diophantine equations $z^2 = f(x)^2 \pm f(y)^2$ involving quartic polynomials." Periodica Mathematica Hungarica 79, no. 1 (2019) : 25-31.